RS220xK

A. Configuration

A.1 This Page is Intentionally Blanked ····· CONF 01-0000
A.2 Explanation of Node ····· CONF 02-0000
A.3 This Page is Intentionally Blanked ····· CONF 03-0000
A.4 Installing the Nodes ····· CONF 04-0000

B. Setting / Display

B.1 Connection and Confirmation of OS Console ····· STDP 01-0000
B.2 BIOS Setting ····· STDP 02-0000
B.3 Maintenance CLI ····· STDP 03-0000
B.4 Setting Value when the OS is Installed ····· STDP 04-0000
B.5 Disk Setting ····· STDP 05-0000

C. Platform Specified Troubleshooting

C.1 Local Initial Operations According to Maintenance Request ····· PSTR 01-0000
C.2 Failure Determination Procedure ····· PSTR 02-0000
C.3 Messages ····· PSTR 03-0000

D. Platform Specified Replace

D.1 Replacing the Components ····· PSRP 01-0000
D.2 Appendix.A A Node Replacement Procedure ····· PSRP 02-0000

Copyright © 2011, 2015, Hitachi, Ltd.

This page is for editorial purpose only.

Copyright © 2011, Hitachi, Ltd.

CONTENTS

A.1 This Page is Intentionally Blanked

Copyright © 2011, Hitachi, Ltd.

This page is for editorial purpose only.

Copyright © 2011, Hitachi, Ltd.

A.1 This Page is Intentionally Blanked

Copyright © 2011, Hitachi, Ltd.

This page is for editorial purpose only.

Copyright © 2011, Hitachi, Ltd.

CONTENTS

A.2 Explanation of Node

A.2.1 Front side

A.2.1.1 Front side of a node

A.2.2 Back side

A.2.2.1 Power source unit

A.2.2.2 Port arrangement and port names

A.2.3 LAN Cable

A.2.3.1 In the case of cluster configuration

A.2.3.2 In the case of single node configuration

A.2.4 Notes on Port when Maintenance Mode is Used

Copyright © 2011, 2012, Hitachi, Ltd.

This page is for editorial purpose only.

Copyright © 2011, Hitachi, Ltd.

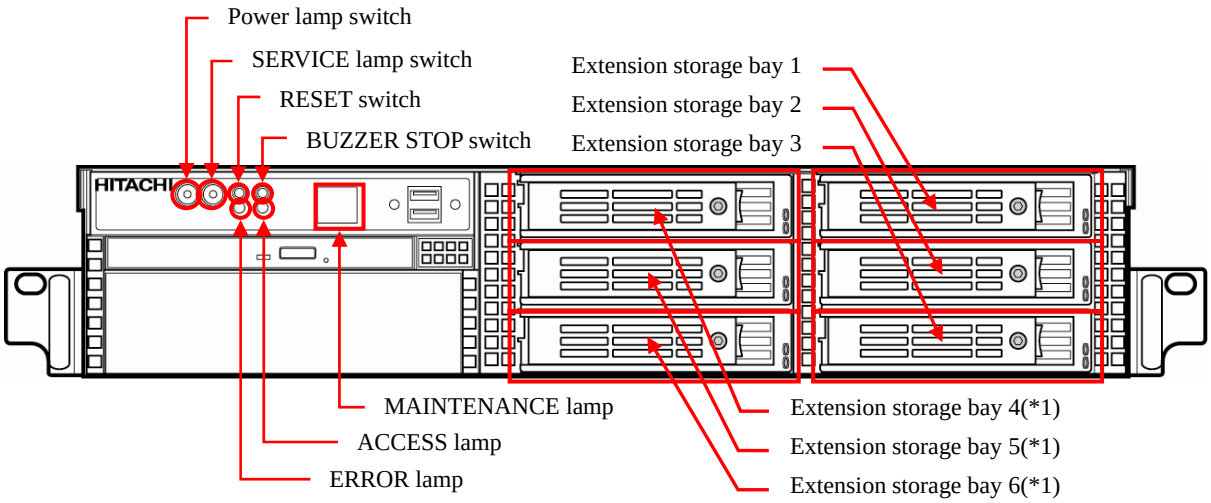
A.2 Explanation of Node

A.2.1 Front side

A.2.1.1 Front side of a node

Figure A.2.1.1-1 shows the front side of a node.
When there is an instruction to press the power source button, press Power lamp switch.

An NMI issue is executed by pressing BUZZER STOP switch and SERVICE lamp switch at the same time.



*1: If the OS version is 3.2.3-XX or later, the number for expansion storage bay will be varied as follows.
- Expansion storage bay “4” is replaced with “5”.
- Expansion storage bay “5” is replaced with “6”
- Expansion storage bay “6” is replaced with “7”

To check the OS version, refer to “Maintenance Tool ‘2.34 Displaying the Version of the OS (versionlist)’ (MNTT 02-2060)”.

Figure A.2.1.1-1 The front side of a node

Copyright © 2011, 2013, Hitachi, Ltd.

A.2.2 Back side

A.2.2.1 Power source unit

Figure A.2.2.1-1 shows the mounted location of the power source unit. And Table A.2.2.1-1 shows the display status of the power source lamp.

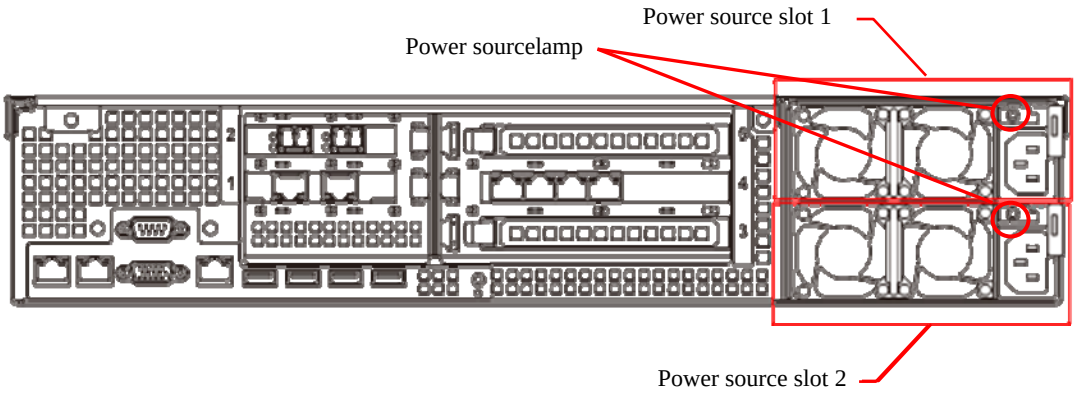


Figure A.2.2.1-1 Location of the mounted power source unit

Table A.2.2.1-1 Display status of the power source lamp of the power source unit

#	Display status of the power source lamp	Operation status
1	Turned off	No AC power supplied (the power source cord is unconnected.)
2	Blinking in green light	AC power supplied and Stand-by status (the power source code is connected, but the power switch is OFF.)
3	Turn on in green	Power ON and the normal operation (Power switch is ON.)
4	Blinking in amber light	An error occurred. (A failure occurred or the power source code is dropped.)

Copyright © 2011, Hitachi, Ltd.

A.2.2.2 Port arrangement and port names

(1) Node in the cluster configuration
Figure A.2.2.2-1 shows the port names on the backside of a node.
When the maintenance tool is used, the port name of the diagram is shown.
'Table A.2.2.2-1 Confirmation Table for the Port Allocation of Node' shows the correspondence between the port names displayed on the maintenance CLI (names on the OS) and the actual port positions of a node.
And (a) to (c) show the rear view of the node in each option card mounting pattern (3 patterns). The extension slots from 1 to 3 are fixed.

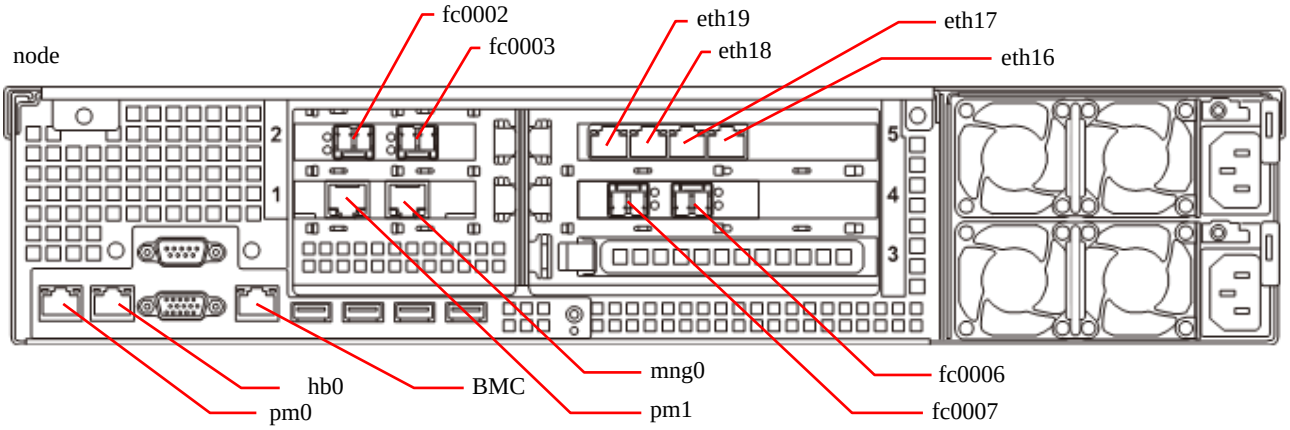


Figure A.2.2.2-1 Rear View of the Node (Example)

Copyright © 2011, 2012, Hitachi, Ltd.

Table A.2.2.2-1 Confirmation Table for the Port Allocation of Node

#	Position	Port position	Interface name		Application	Remarks
			GbE	FC		
1	On-board	1	hb0		heartbeat port	
2		2	pm0		Private Maintenance port	
3		M	— (none)		BMC	
4	Extension slot 1	1	mng0		Management port	PCI-Express 2.0<×4>
5		2	pm1		Reserved port	
6	Extension slot 2	0		fc0002	Connecting an FC port and the disk array subsystem	PCI-Express 2.0<×4>
7		1		fc0003	Connecting an FC port and the disk array subsystem	
8	Extension slot 3	1			unused	
9		2				
10		3				
11		4				
12	Extension slot 4	0	eth12	fc0006	data port Connecting an FC port and the disk array subsystem	PCI-Express 2.0<×8>
13		1	eth13	fc0007	data port Connecting an FC port and the disk array subsystem	
14		2	eth14		data port	
15		3	eth15		data port	
16	Extension slot 5	0	eth16		data port	PCI-Express 2.0<×8>
17		1	eth17		data port	
18		2	eth18		data port	
19		3	eth19		data port	

Copyright © 2011, 2012, Hitachi, Ltd.

The following shows the three built-in patterns by the combination of the option card.

(a) Mounting 4 port GbE card in the extension slot 4

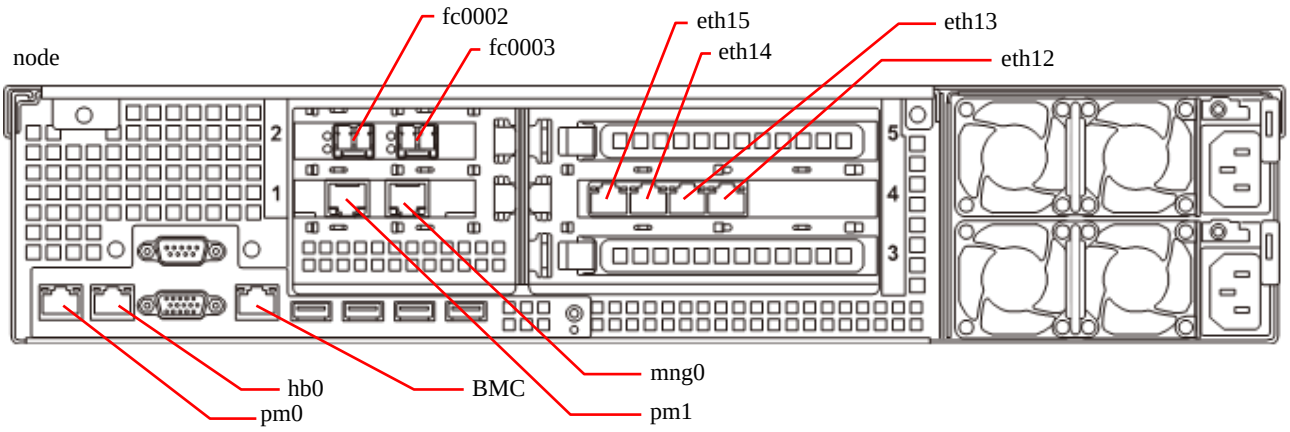


Figure A.2.2.2-2 Rear View of the Node (1)

(b) Mounting 4 port GbE card in the extension slot 4 and the extension slot 5

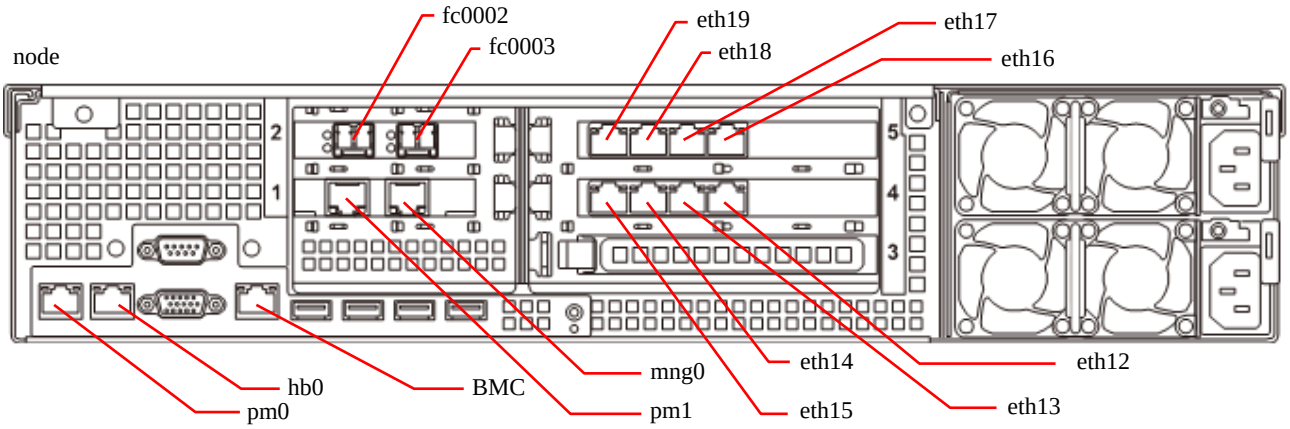


Figure A.2.2.2-3 Rear View of the Node (2)

Copyright © 2011, Hitachi, Ltd.

(c) Mounting 2 port FC card in the extension slot 4 and mounting 4 port GbE card in the extension slot 5

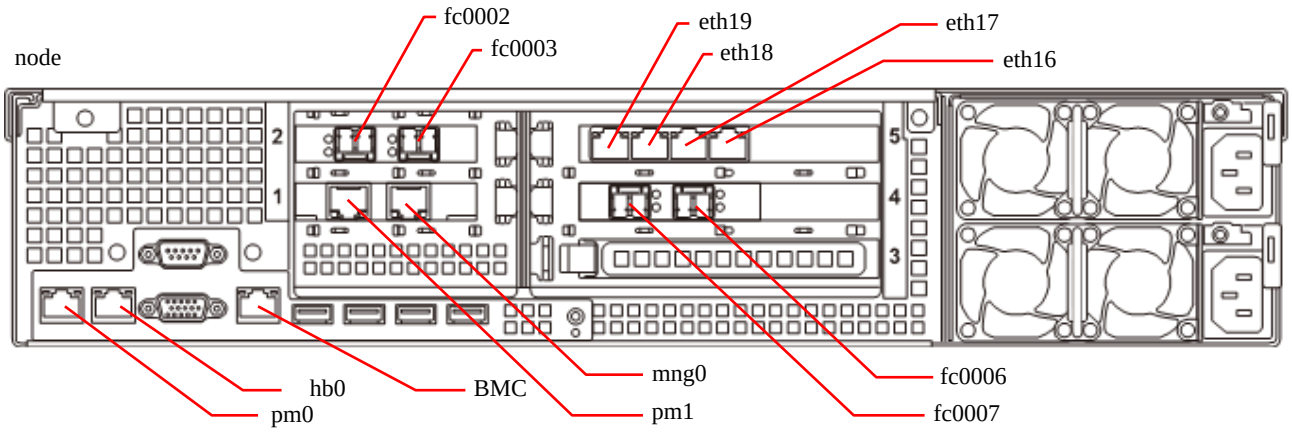


Figure A.2.2.2-4 Rear View of the Node (3)

Copyright © 2011, Hitachi, Ltd.

(2) Node in the single node configuration
Figure A.2.2.2-5 shows the port names on the backside of a node.
When maintenance tool is used, the port name of the diagram is shown.
Table A.2.2.2-2 shows the correspondence between the port names displayed on the maintenance CLI (names on the OS) and the actual port positions of a node.

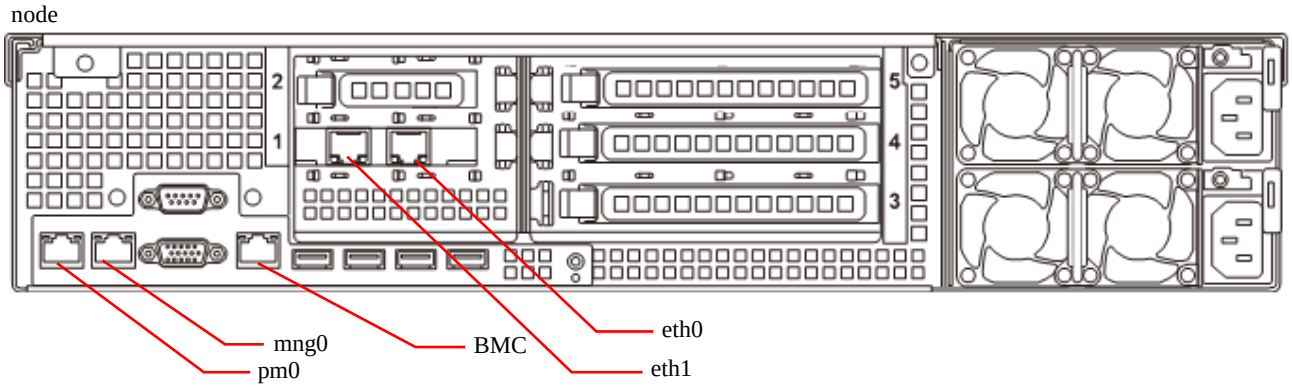


Figure A.2.2.2-5 Rear View of the Node

Table A.2.2.2-2 Confirmation Table for the Port Allocation of Node

#	Position	Port position	Interface name	Application	Remarks
1	On-board	1	pm0	Private Maintenance port	—
2		2	mng0	Management port	It is also used for the connection to Front-end LAN.
3		BMC	bmc0	BMC	—
4	Extension slot 1	3	eth0	data port	It becomes unused port when the management port connects to Front-end LAN.
5		4	eth1	data port	

Copyright © 2011, Hitachi, Ltd.

A.2.3 LAN Cable

NOTE: When using the customer's management LAN IP-SW, request the customer to connect the connections of #1 to #4 of Management VLAN ports shown in the Figure A.2.3.1-1 to the 4 of 6 ports provided by the customer.

A.2.3.1 In the Case of Cluster Configuration shows the LAN cable connection when it is cluster configuration, and 'A.2.3.2 In the case of single node configuration' shows when it is single node configuration.

A.2.3.1 In the case of cluster configuration

Note that No. 9 port of the management LAN IP-SW is unoccupied port because it is an alternative port for No.1 or No.3 port of the Management LAN IP-SW in case when problem occurs.
However, if the No.9 port is occupied with the use of HiTrack, No.8 port is used as an alternative port.

Copyright © 2011, 2012, Hitachi, Ltd.

(1) Connecting the management system network

Connect the management port (mng) of node0 to port 1 on the management LAN IP-SW, and connect the BMC of node0 to port 2 on the management LAN IP-SW.
Connect the management port (mng) of node1 to port 3 on the management LAN IP-SW, and connect the BMC of node1 to port 4 on the management LAN IP-SW.
Connect the management server to port 7 on the management LAN IP-SW.

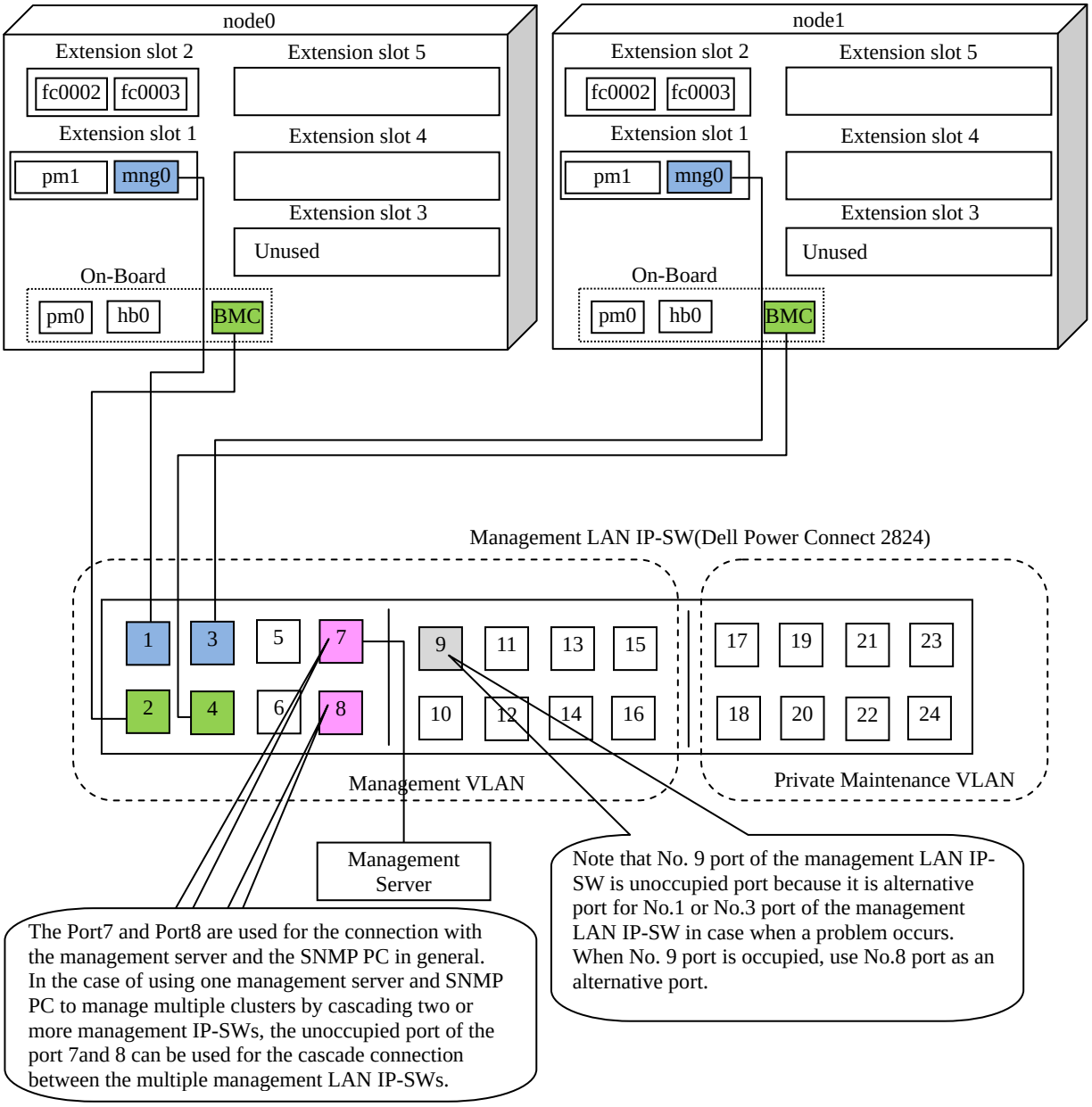


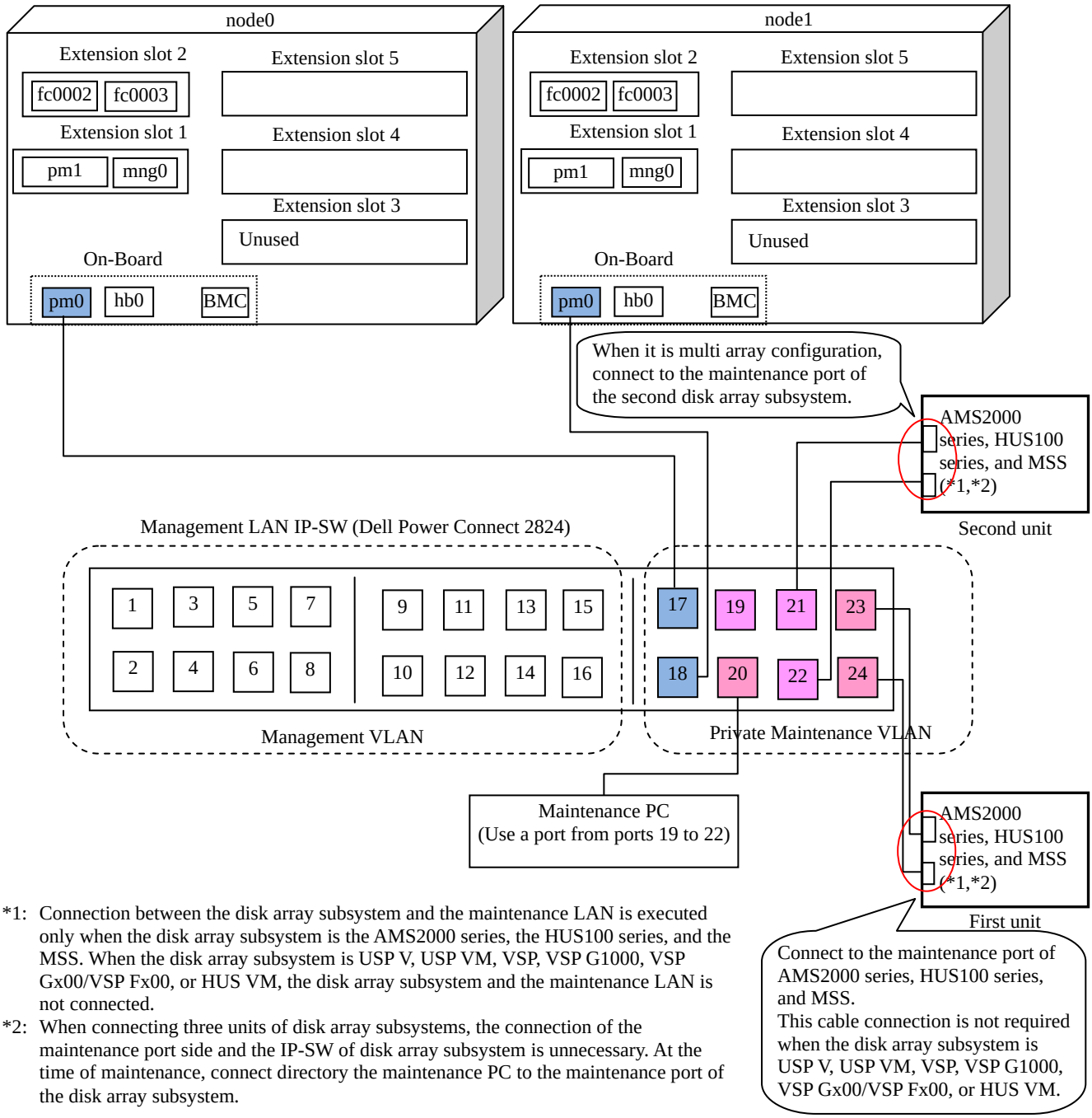
Figure A.2.3.1-1 Connection Diagram for the Management System Network

Copyright © 2011, 2014, Hitachi, Ltd.

(2) Connecting the private maintenance ports

NOTE: This connection is unnecessary when the customer's management LAN IP-SW is used.

Connect the private maintenance port (pm) of node0 to port 17 on the management LAN IP-SW.
Connect the private maintenance port (pm) of node1 to port 18 on the management LAN IP-SW.
When you use a maintenance PC, connect it to a free port from ports 19 to 22 on management LAN IP-SW.



*1: Connection between the disk array subsystem and the maintenance LAN is executed only when the disk array subsystem is the AMS2000 series, the HUS100 series, and the MSS. When the disk array subsystem is USP V, USP VM, VSP, VSP G1000, VSP Gx00/VSP Fx00, or HUS VM, the disk array subsystem and the maintenance LAN is not connected.

*2: When connecting three units of disk array subsystems, the connection of the maintenance port side and the IP-SW of disk array subsystem is unnecessary. At the time of maintenance, connect directory the maintenance PC to the maintenance port of the disk array subsystem.

Figure A.2.3.1-2 Private Maintenance Port Connection Diagram

Copyright © 2011, 2016, Hitachi, Ltd.

(3) Connecting the heartbeat ports

Connect the heartbeat ports (hb) of nodes 0 and 1.
For the LAN cable to connect the heartbeat port, the 5E or more categories is required.

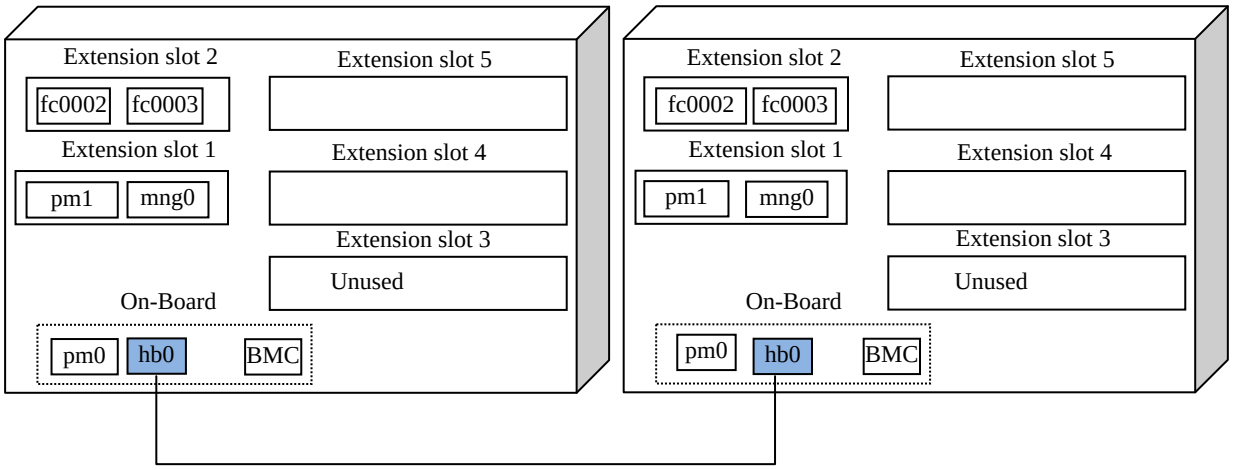


Figure A.2.3.1-3 Heartbeat Port Connection Diagram

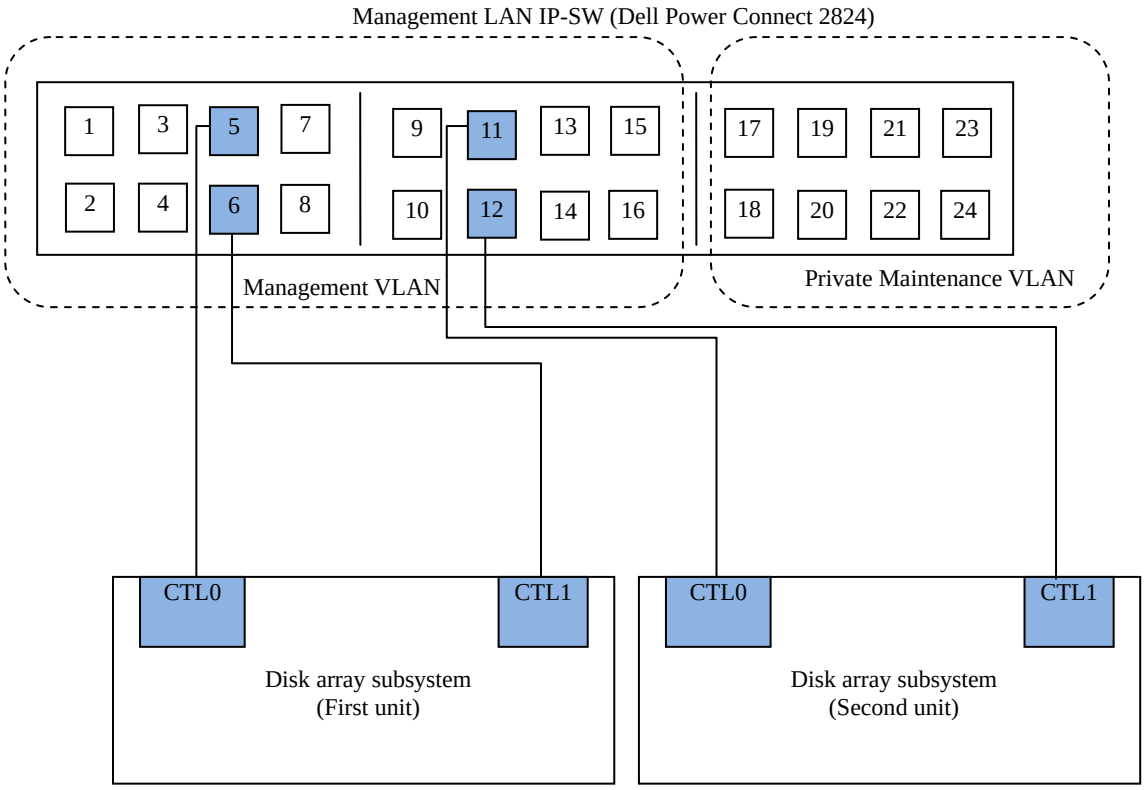
Copyright © 2011, Hitachi, Ltd.

(4) Connecting the management LAN IP-SW and the disk array subsystem

Disk array subsystems are connected to the management LAN only for the AMS2000 series or HUS100 series. They are not necessary to be connected to the management LAN for USP V, USP VM, VSP, VSP G1000, or VSP Gx00/VSP Fx00. If disk array subsystems are connected, connect them to #5 or #6.

Connect ports 5 and 6 on the management LAN IP-SW to the user management port (LAN1) on the disk array subsystem (first unit).
When connecting one more disk array subsystem, connect the disk array subsystem to the port 11 and 12 on the management LAN IP-SW. When connecting third unit of disk array subsystem, apply cascade connection by connecting the disk array subsystem to the port 13 and 14 or add an IP-SW or connect the disk array subsystem to the port 15 and 16 if the port 15 and 16 on the management VLAN are unoccupied.

NOTE: When using the customer's management LAN IP-SW, request the customer to connect the connections of #5 to #6 of Management VLAN ports shown in the Figure A.2.3.1-4 to the 2 of 6 ports provided by the customer.



Copyright © 2011, 2016, Hitachi, Ltd.

(5) Connecting the front-end LAN

NOTE: When using the HiTrack in the configuration of HDI for HCP, the customer's Management LAN IP-SW and front-end LAN are needed to be connected.

Connect port 10 on the management LAN IP-SW to the router.
Connect the router to the front-end LAN.
Router is connected only when the system environment is the configuration of HDI for HCP, and a customer makes a contract of Hi-Track with HDS.

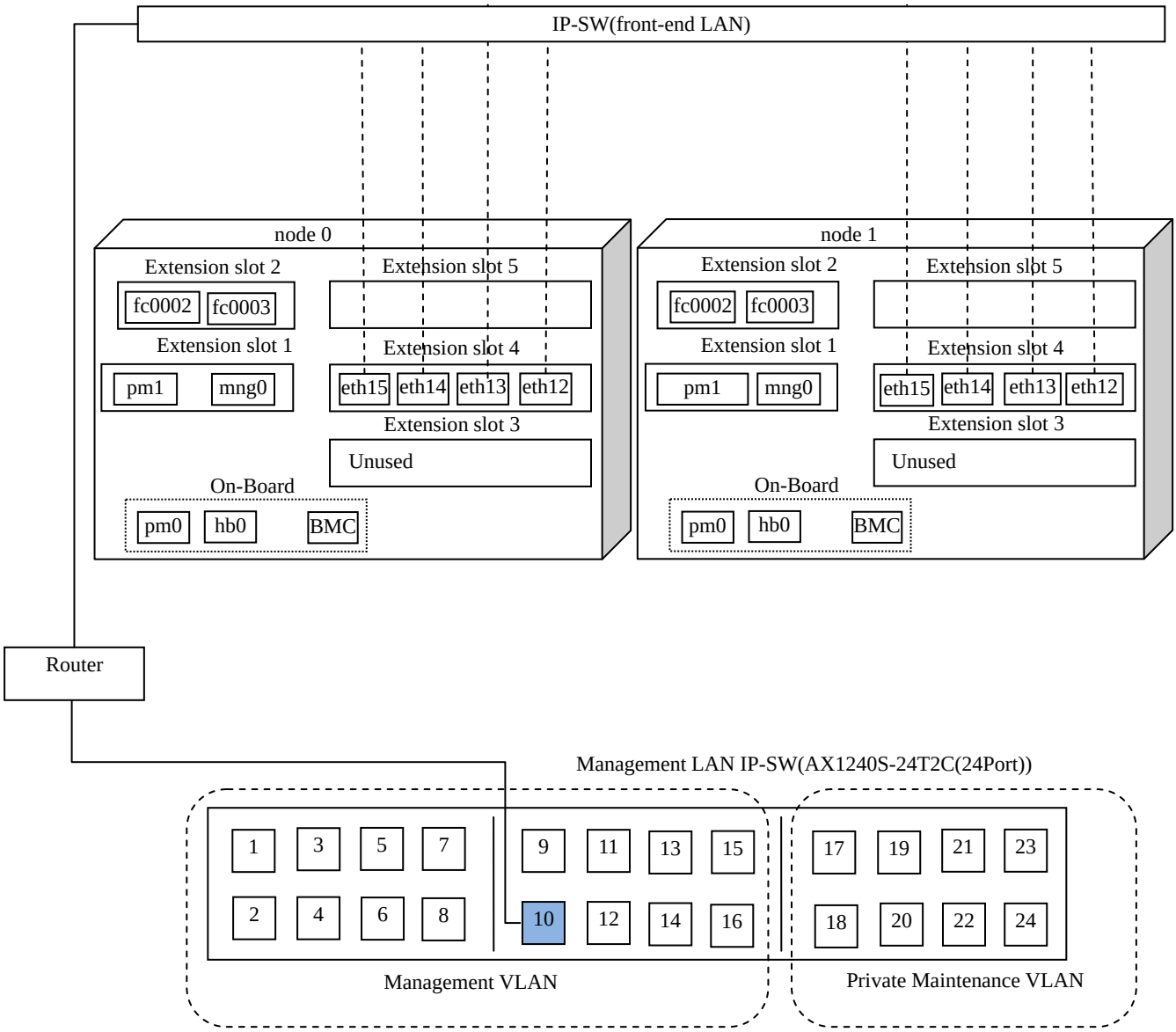


Figure A.2.3.1-5 Front-end LAN Connection Diagram

Copyright © 2011, 2012, Hitachi, Ltd.

(6) Connecting the HiTrack PC

NOTE: When using the customer's management LAN IP-SW, request the customer to connect the HiTrack PC to the customer's management LAN IP-SW.

Figure A.2.3.1-6 shows the HiTrack PC connection diagram. (Either HiTrack or SNMP is required.)

Connect the HiTrack PC to port 9 on the management LAN IP-SW.
When you use SNMP, connect it to port 8 on the management LAN IP-SW.

HiTrack monitors HDI via the management LAN.
It also monitors the HCP node via the connection with the front-end LAN described in (5).

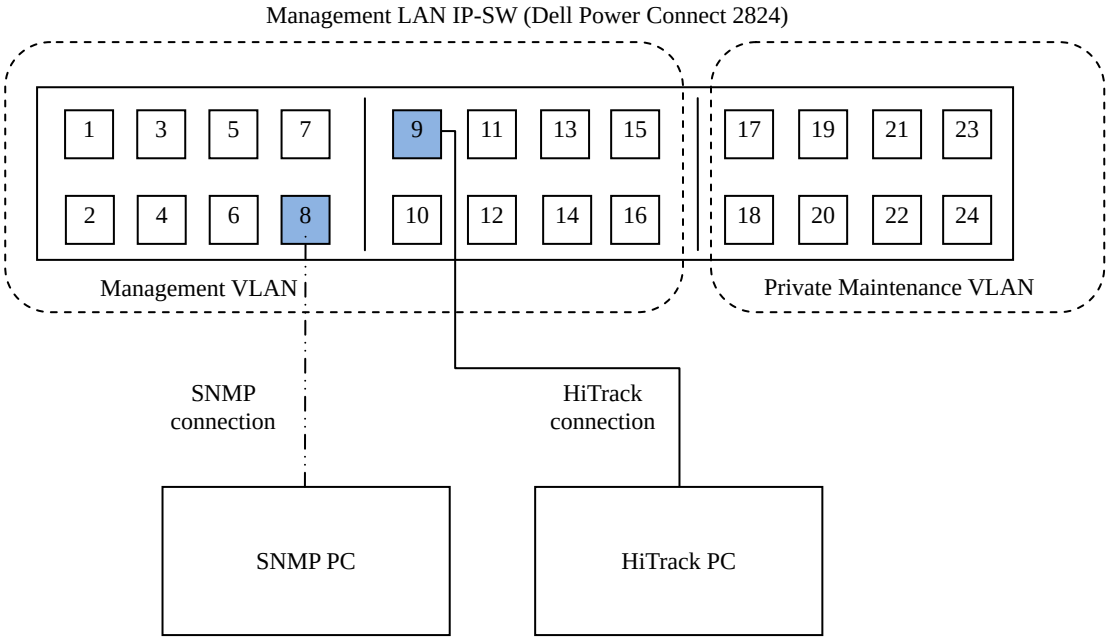


Figure A.2.3.1-6 HiTrack PC Connection Diagram

Copyright © 2011, 2012, Hitachi, Ltd.

A.2.3.2 In the case of single node configuration

(1) Connecting the front-end LAN
Figure A.2.3.2-1 shows a case of front-end LAN connection by using the two LAN cable, and Figure A.2.3.2-2 shows a case of front-end LAN by using the one LAN cable.

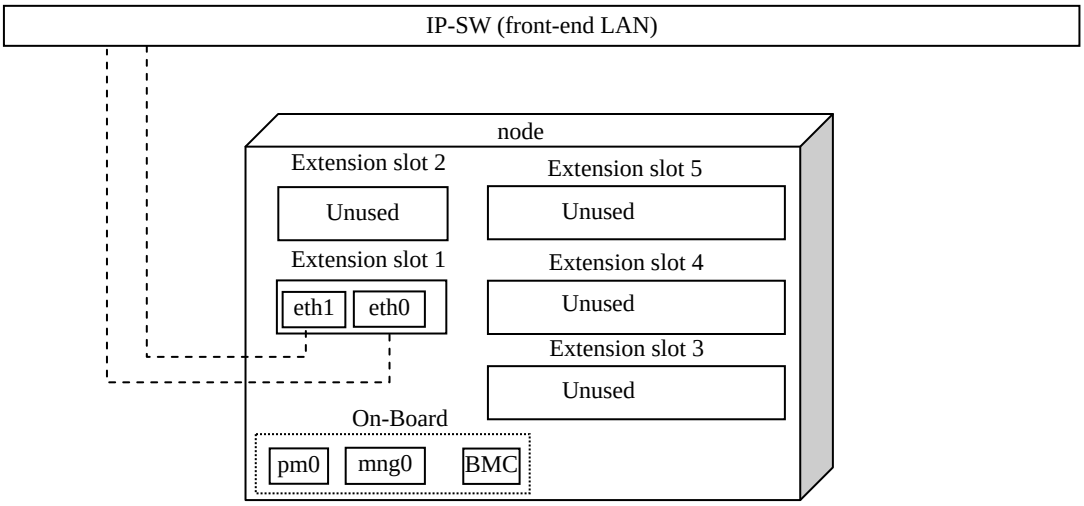


Figure A.2.3.2-1 Front-end LAN Connection by using two LAN cables (Configuration using trunk 2 Data ports)

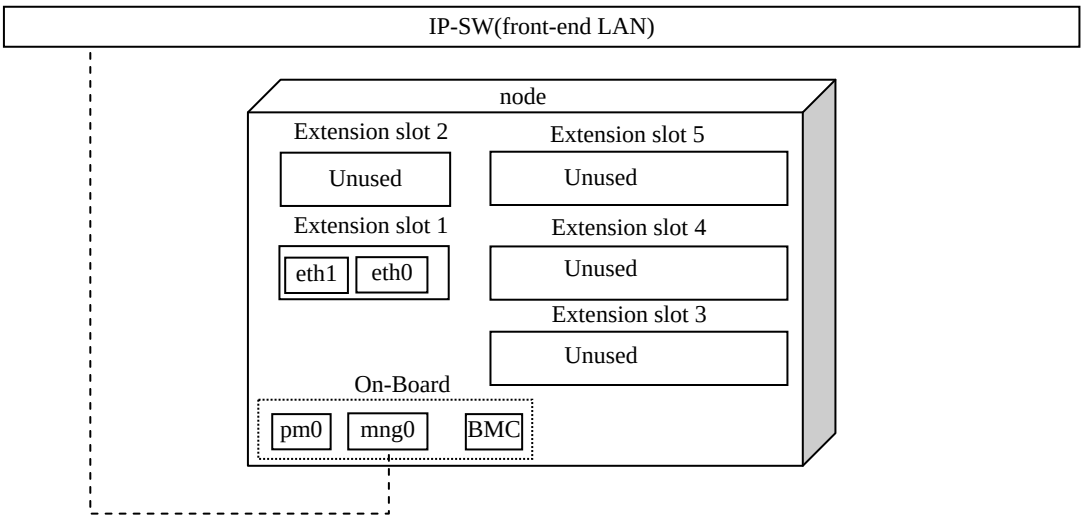


Figure A.2.3.2-2 Front-end LAN Connection by using one LAN cable (Configuration using Management port)

(2) Connecting the private maintenance ports

Private Maintenance port should be connected directly with a maintenance PC.

Copyright © 2011, Hitachi, Ltd.

A.2.4 Notes on Port when Maintenance Mode is Used

This is unsupported mode in this model.

Copyright © 2011, Hitachi, Ltd.

CONTENTS

A.3 This Page is Intentionally Blanked

Copyright © 2011, Hitachi, Ltd.

This page is for editorial purpose only.

Copyright © 2011, Hitachi, Ltd.

A.3 This Page is Intentionally Blanked

Copyright © 2011, 2012, Hitachi, Ltd.

This page is for editorial purpose only.

Copyright © 2011, 2012, Hitachi, Ltd.

CONTENTS

A.4 Installing the Nodes

A.4.1 Example of Installing the Node in the Basic Configuration (cluster node)

A.4.2 Example of Installing the Node in the Basic Configuration (single node)

A.4.3 Example of Installing the Node in the Configuration of HDI for HCP (cluster node)

A.4.4 Example of Installing the Node in the Configuration of HDI for HCP (single node)

A.4.5 Example of Installing the Node in the Configuration of HDI for Cloud (cluster node)

A.4.6 Example of Installing the Node in the Configuration of HDI for Cloud (single node)

Copyright © 2011, 2012, Hitachi, Ltd.

This page is for editorial purpose only.

Copyright © 2011, Hitachi, Ltd.

A.4 Installing the Nodes

A.4.1 Example of Installing the Node in the Basic Configuration (cluster node)

HDI does not support Basic Configuration.

Copyright © 2011, 2012, Hitachi, Ltd.

A.4.2 Example of Installing the Node in the Basic Configuration (single node)

HDI does not support Basic Configuration.

Copyright © 2012, Hitachi, Ltd.

A.4.3 Example of Installing the Node in the Configuration of HDI for HCP (cluster node)

CAUTION

To prevent a rack frame fall, install the heavier devices on the lower positions as much as possible. The devices must be installed in the order of a position from the bottom. Please make sure when you install nodes on your rack frame.

The following figure shows an example of installing the nodes of Hitachi Data Ingestor on a rack on which the Hitachi Content Platform has been installed.
Installing Hitachi Data Ingestor requires a 6U rack space. Figure A.4.3-1 shows an example of installing the basic chassis of AMS2000 series and three extension chassis mounted from the bottom of the rack frame. In this case, totally 13U rack spaces are required with the basic chassis and three extension chassis.
When connecting with USP V, USP VM, or VSP, the disk array subsystem will not be installed on a rack frame of which the node is installed.

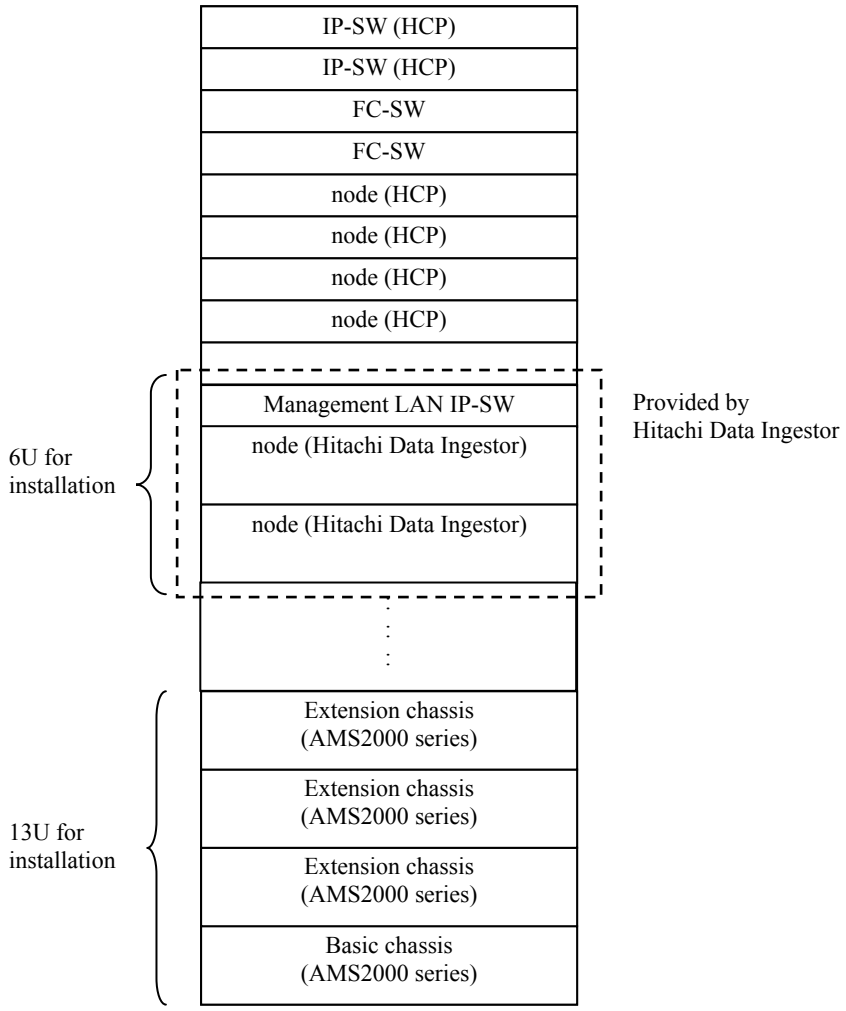


Figure A.4.3-1 Example of Installing the node in the Configuration of HDI for HCP

Copyright © 2011, 2016, Hitachi, Ltd.

A.4.4 Example of Installing the Node in the Configuration of HDI for HCP (single node)

CAUTION

To prevent a rack frame fall, install the heavier devices on the lower positions as much as possible. The devices must be installed in the order of a position from the bottom. Please make sure when you install nodes on your rack frame.

The following figure shows an example of installing the nodes of Hitachi Data Ingestor on a rack on which the Hitachi Content Platform has been installed.
There are no Management LAN IP-SW, Array Storage, and KVM in HDI single node configuration, so HDI needs only 2U for one Dell/PowerEdge R710.
Figure A.4.4-1 shows an example of installing the basic chassis and 3 extended chassis of AMS2000 in the order of a position from the bottom.

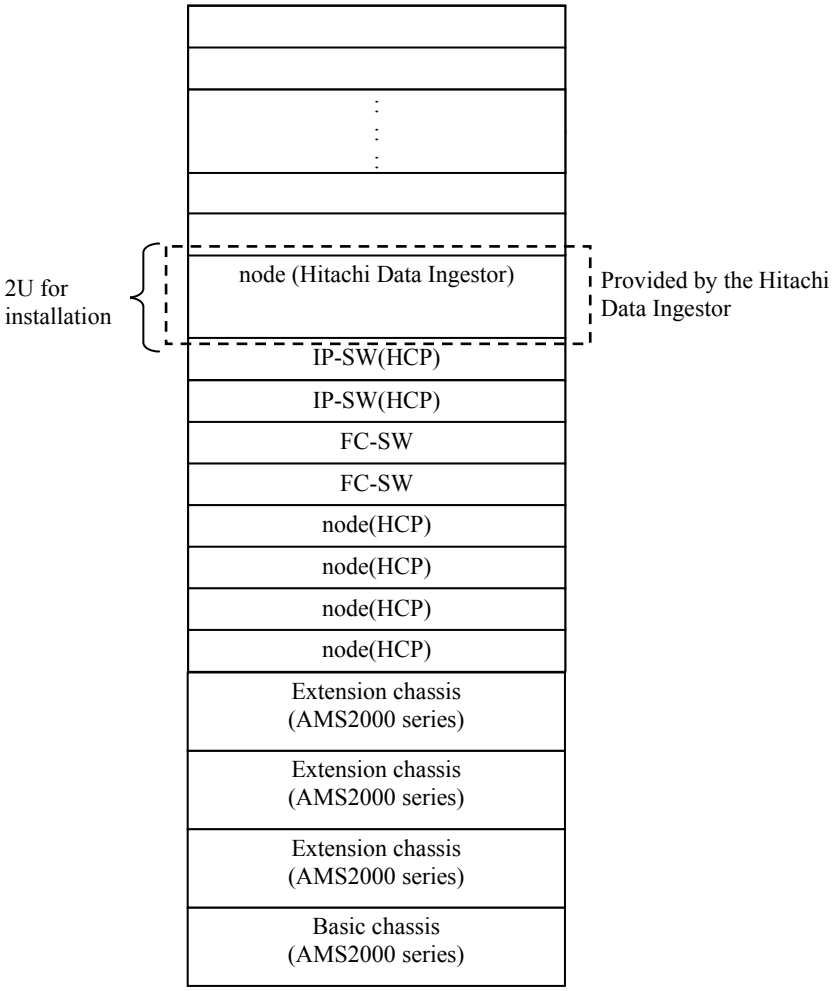


Figure A.4.4-1 Example of Installing the node in the Configuration of HDI for HCP (single node)

Copyright © 2011, 2016, Hitachi, Ltd.

A.4.5 Example of Installing the Node in the Configuration of HDI for Cloud (cluster node)

CAUTION

To prevent a rack frame fall, install the heavier devices on the lower positions as much as possible. The devices must be installed in the order of a position from the bottom. Please make sure when you install nodes on your rack frame.

The disk array subsystem in the figure shows an example with AMS2000 series.

Figure A.4.5-1 shows an example of installing the nodes of HDI for Cloud configuration (cluster node).

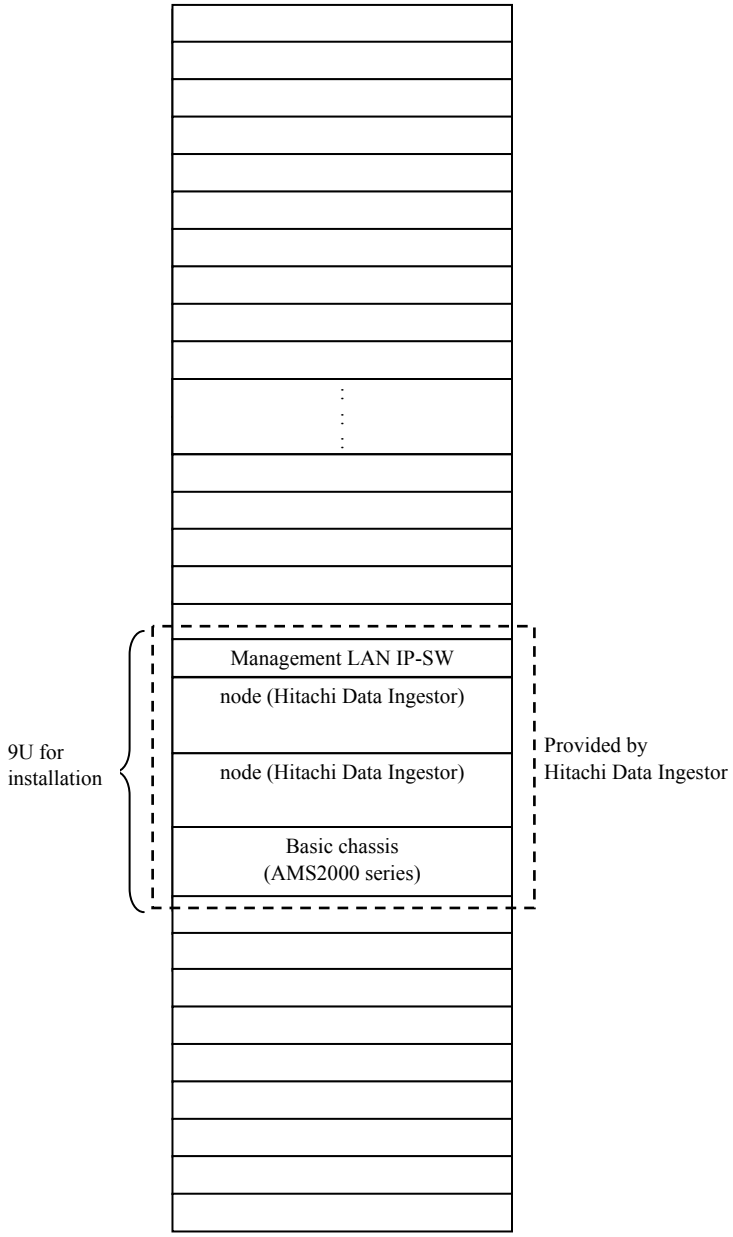


Figure A.4.5-1 Example of Installing the node in the Configuration of HDI for Cloud (cluster node)

Copyright © 2011, 2016, Hitachi, Ltd.

A.4.6 Example of Installing the Node in the Configuration of HDI for Cloud (single node)

CAUTION

To prevent a rack frame fall, install the heavier devices on the lower positions as much as possible. The devices must be installed in the order of a position from the bottom. Please make sure when you install nodes on your rack frame.

Install only a node in the configuration of HDI for Cloud (single node) because any of disk array subsystem, maintenance LAN, IP-SW, KVM is not used for this configuration.

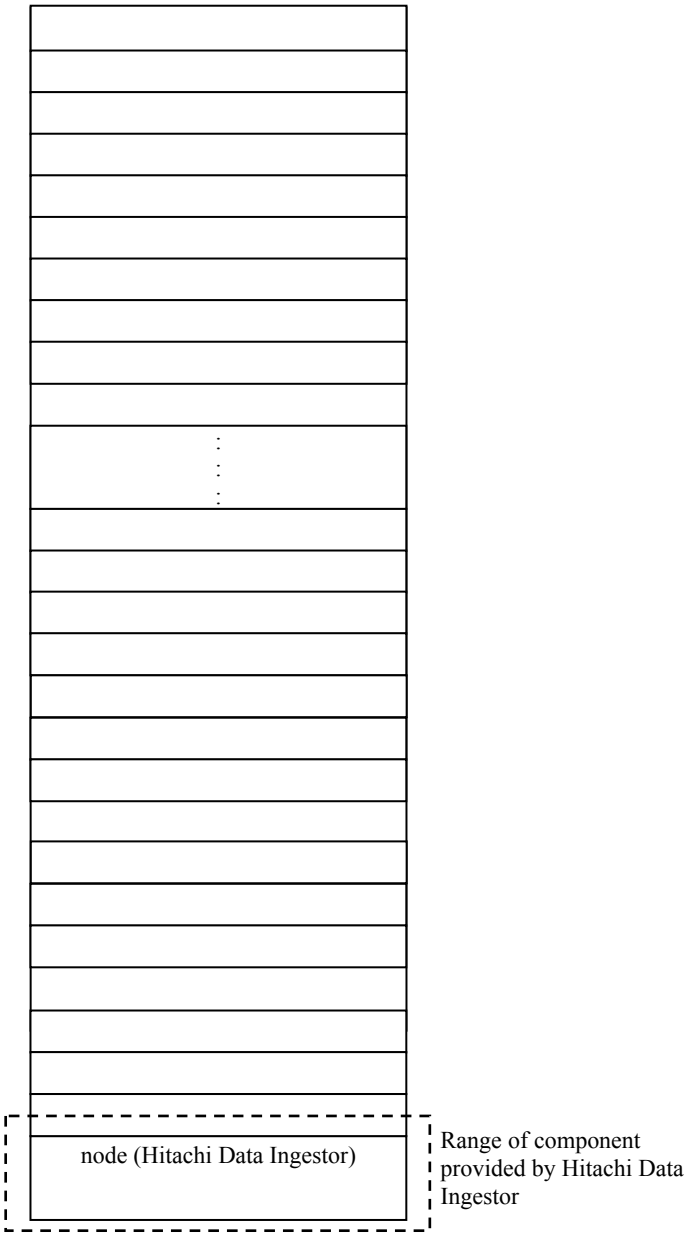


Figure A.4.6-1 Example of installing the node of the configuration of HDI for Cloud (single node)

Copyright © 2011, 2016, Hitachi, Ltd.

CONTENTS

B.1 Connection and Confirmation of OS Console

B.1.1 Confirmation of KVM Connection

B.1.2 Startup Confirmation of the OS by Using KVM

B.1.3 Connection Confirmation of the Remote Console

B.1.4 Startup Confirmation of OS by Using Remote Console

Copyright © 2011, Hitachi, Ltd.

This page is for editorial purpose only.

Copyright © 2011, Hitachi, Ltd.

B.1 Connection and Confirmation of OS Console

There are two methods of connection to the console of OS. One is the connection with KVM, and the other is the connection with remote console.

KVM is an input/output device with a hardware display monitor, and the command operation for the node can be executed. Generally, KVM can connect to multiple nodes and it uses by switching nodes. Note that KVM is not used in this model.

Remote Console is a function that can be executed a command operation for the node on a screen of a maintenance PC by installing the remote console application to the maintenance PC. Remote console uses in the case other than installation operation and BMC failures.

For more details about Remote Console Application, refer to “Remote Console Application User’s Guide for HA8000xK System”.

B.1.1 Confirmation of KVM Connection

Refer to ‘B.1.3 Connection Confirmation of the Remote Console’ in this model.

B.1.2 Startup Confirmation of the OS by Using KVM

Refer to ‘B.1.4 Startup Confirmation of OS by Using Remote Console’ in this model.

Copyright © 2011, Hitachi, Ltd.

B.1.3 Connection Confirmation of the Remote Console

NOTE: In the case of BMC port failure, borrow a monitor and a keyboard from the system administrator to connect to the node.

The console must be available to use before executing setup operation. Confirm that the following descriptions are connected certainly.

(1) Verify that the power source cable of the maintenance PC is connected.
(2) Verify that the network segment of the BMC port and the network segment of the maintenance PC are the same.

If the network segment is different, change the setting of maintenance PC to be the same network segment. The following shows the conceivable IP address of the BMC port.

- Before the setup, the IP address may be 192.168.100.100.
- After the setup, the IP address may be the following.

[Cluster configuration]
[node0] is [192.168.0.22], and [node1] is [192.168.0.23].

[Single node configuration]
The IP address of the maintenance port is the same segment with the one that specified during installing, and the host part is fixed as 40.
For example, when the IP address of the maintenance port is 10.0.0.51, the IP address of the BMC port is 10.0.0.40.

If the IP address of the BMC port is other than the above IP address, confirm with the system administrator.

(3) Verify that the LAN port of the maintenance PC and the BMC port of the node are connected with a LAN cable (cross-cable).

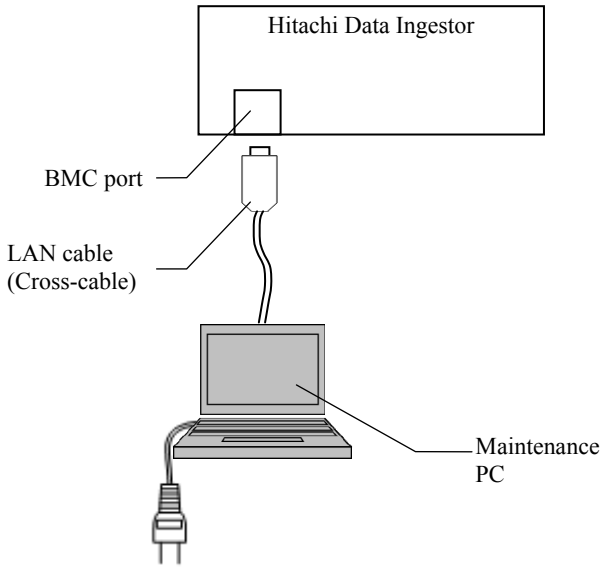


Figure B.1.3-1 Remote console connection example

Copyright © 2011, 2012, Hitachi, Ltd.

B.1.4 Startup Confirmation of OS by Using Remote Console

If the OS is already installed, it is available to check if the OS is running or not with using the console window.

This procedure assumes that the connection confirmation of the console with the description of ‘B.1.3 Connection Confirmation of the Remote Console’.

The following shows the procedure.

(1) Start up the Internet Explorer from the maintenance PC.
Click [Start]-[Program]-[Internet Explorer].

(2) Input the following address in the address bar on the Internet Explorer.
“http://<IP address of the BMC>”

Input the IP address confirmed at ‘B.1.3 Connection Confirmation of the Remote Console’ for the IP address of the BMC.

(3) Make sure that the BMC login window is displayed.

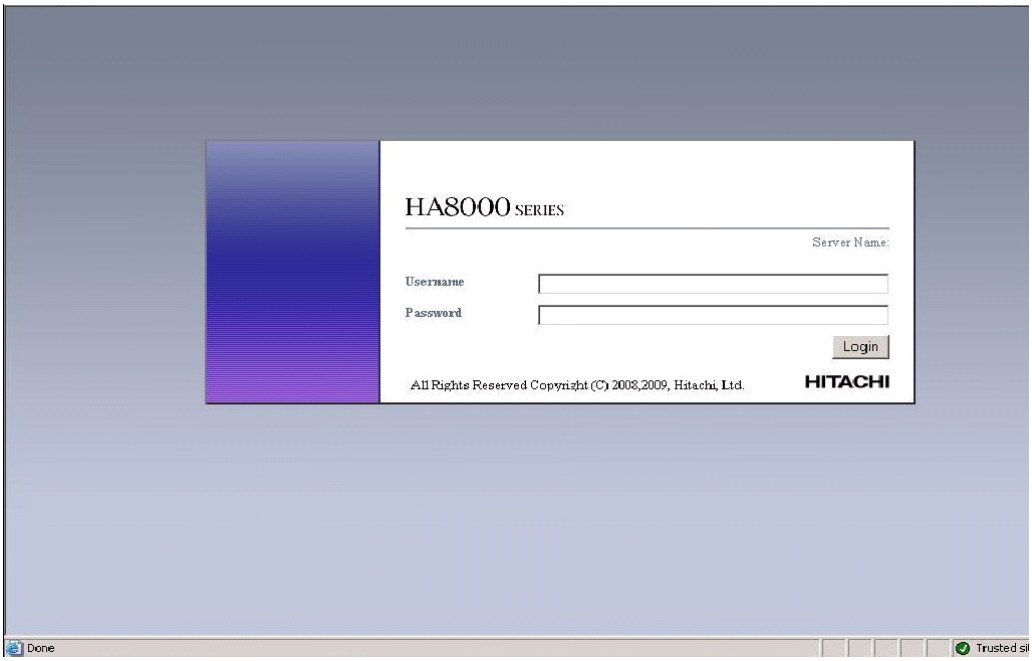


Figure B.1.4-1 BMC Login window 1

Copyright © 2011, 2015, Hitachi, Ltd.

(4) Enter “ceconsl” in the [Username], and “cepasswd” in the [Password].
After the input, click [Login].

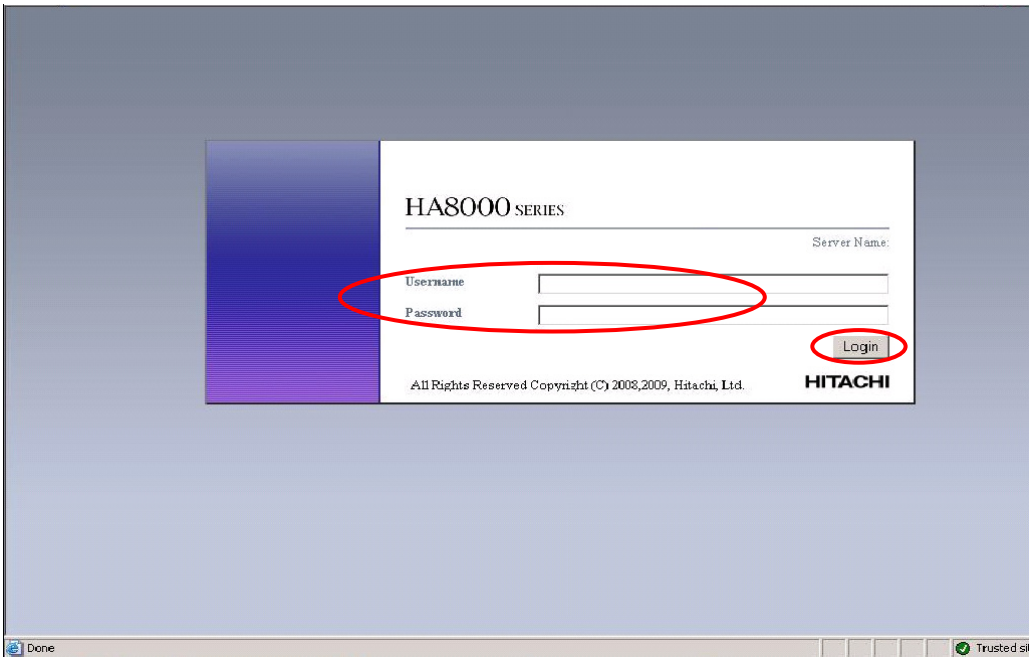


Figure B.1.4-2 BMC Login window 2

(5) The Server Information window is displayed as shown in Figure B.1.4-3.
Click [Server Settings].

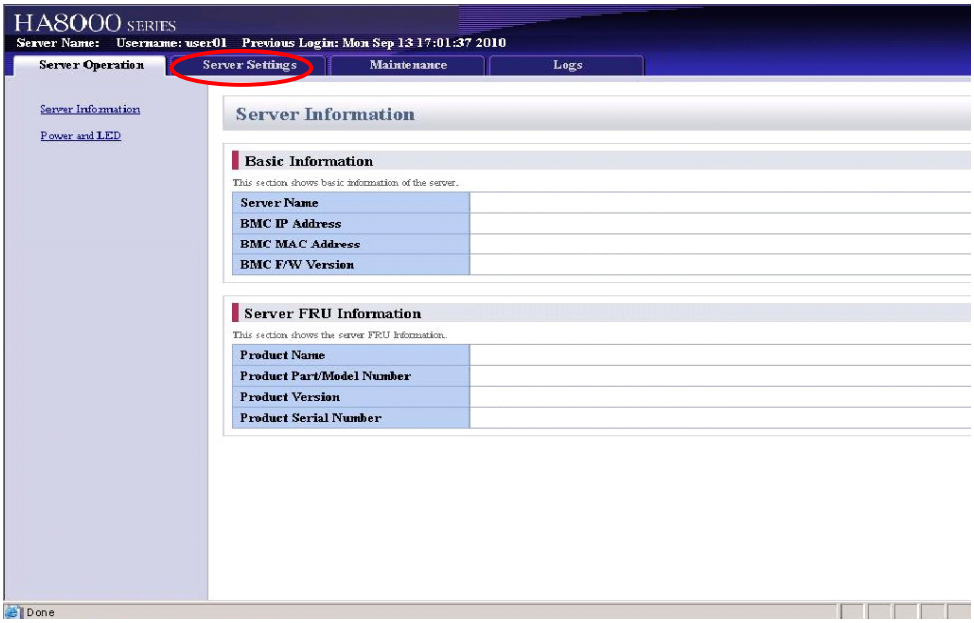


Figure B.1.4-3 Server Information window

Copyright © 2011, 2014, Hitachi, Ltd.

(6) The Language Settings window is displayed as shown in Figure B.1.4-4.
Click [Remote KVM].

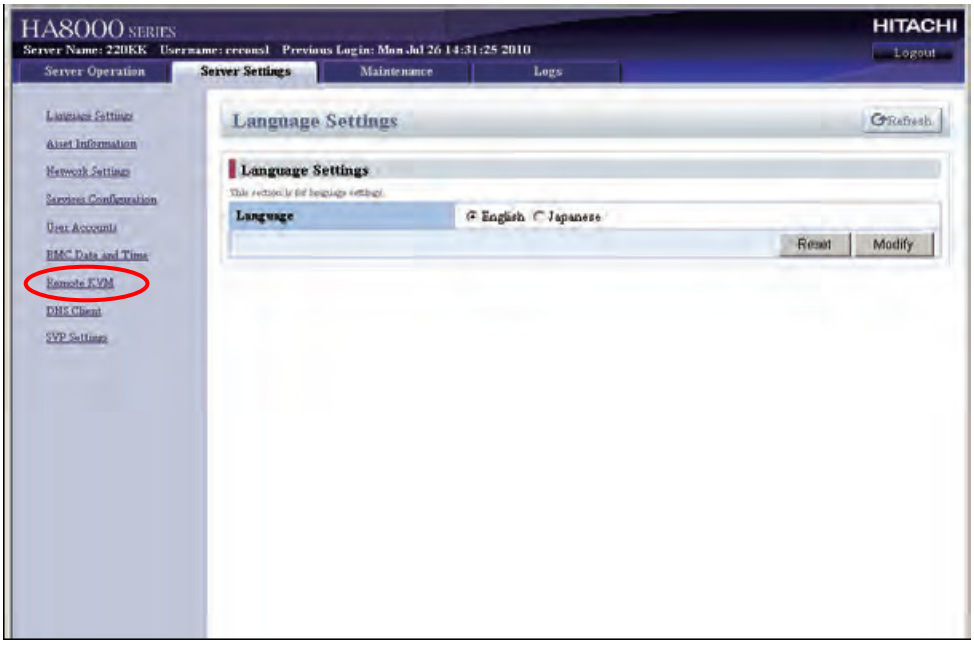


Figure B.1.4-4 Language Settings window

(7) The Remote KVM Settings window is displayed as shown in Figure B.1.4-5.
Select [RELATIVE Mode], and click [Modify].

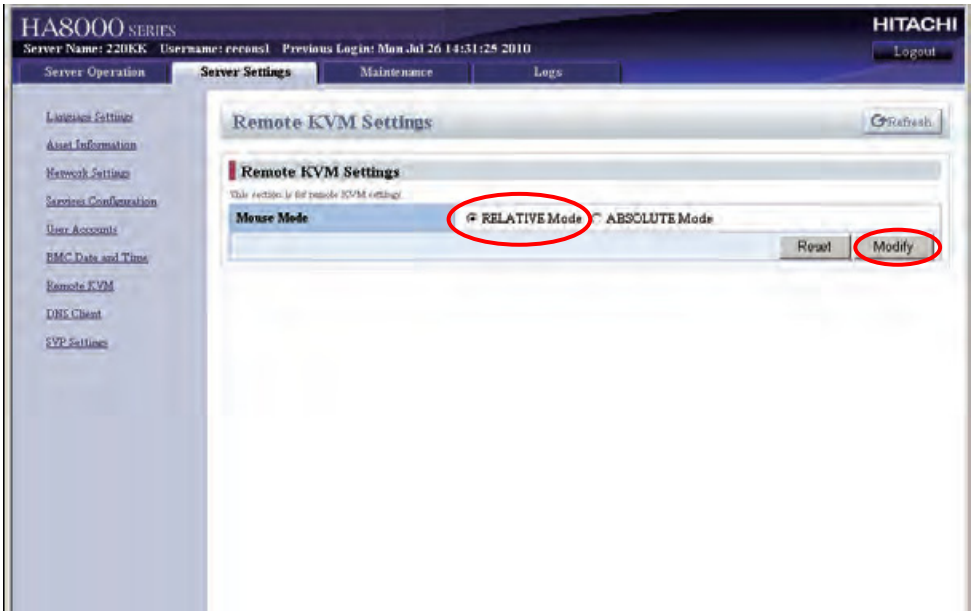


Figure B.1.4-5 Remote KVM Settings window

(8) Click [Logout].

Copyright © 2011, Hitachi, Ltd.

(9) Check if a shortcut icon of “Remote Console” is existed on the desktop of the maintenance PC.
If it exists, proceed to step (10).
If it does not exist, install the remote console application with reference to the “Remote Console Application User’s Guide for HA8000xK System,” and proceed to step (10).

Figure B.1.4-6 Desktop1

(10) Double click the shortcut icon of “Remote Console”.

Figure B.1.4-7 Desktop2

Copyright © 2011, Hitachi, Ltd.

(11) Figure B.1.4-8 Remote Console window is displayed.
Refer to the setting information as shown in B.1.4-1, and input the information into the thick frame, and then click [Connect].

Table B.1.4-1 Configuration Information

#	Item	Setting value
1	IP Address	IP address that is confirmed by 'B.1.3 Connection Confirmation of the Remote Console'.
2	User ID	ceconsl
3	Password	cepasswd
4	Port Number	5001

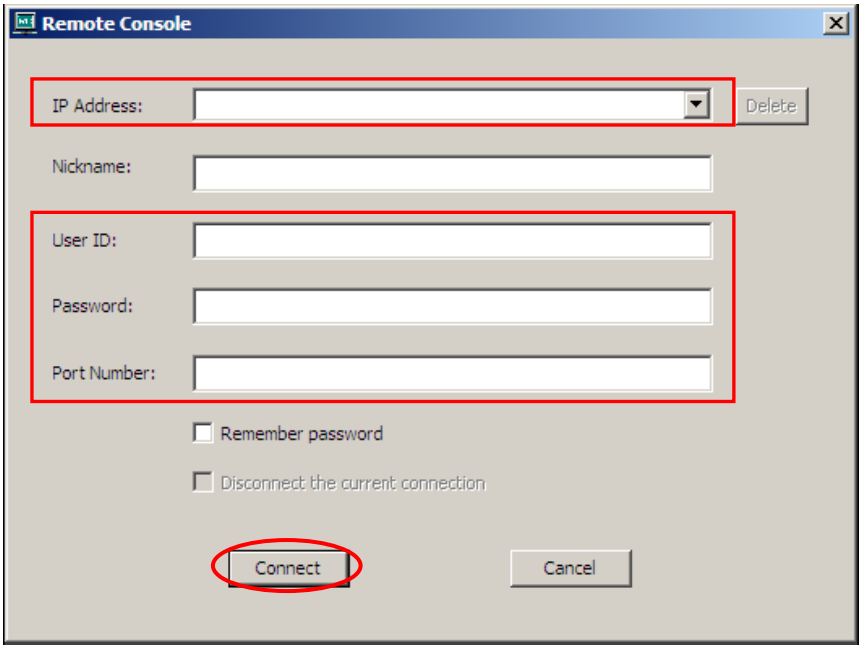


Figure B.1.4-8 Remote Console window

Copyright © 2011, 2014, Hitachi, Ltd.

(12) Confirm that the Console window as shown in Figure B.1.4-9 is displayed.

Figure B.1.4-9 Console window 1

(13) Make sure that Figure B.1.4-10 or Figure B.1.4-11 is displayed. If not displayed, which means either OS is under boot processing / under suspension, or OS has suspended.
If Figure B.1.4-10 has been displayed, go to step (13-1).
If Figure B.1.4-11 has been displayed, go to step (13-2).

(13-1) Press [Enter] key without entering anything in the console window.
Make sure that the same prompt message has been output on the bottom of the login prompt window shown in Figure B.1.4-10.
If the same prompt message is displayed, which means that OS is booting.
If the console window has no response, either OS is hanging up or abnormally stopped.

```
File Operating System (*1)

xxxxxxxx(device-serial-number) login:
```

*1: If the OS version is 3.0.2-XX or earlier, “Hitachi File Storage Linux” is displayed.
Note that “Hitachi File Storage Linux” is not displayed if the version is 3.2.1-XX or later.

Figure B.1.4-10 Login Prompt window

(13-2) Press either [Ctrl] + [F2] key or [Alt] + [F2] key (*) and confirm that the widow has been switched to the login prompt window.
If the window is switched, OS is booting.
If the window is not switched, either OS is hanging up or abnormally stopped.

*: Note that the remote console has the restriction with [Alt] key. Therefore, execute the following three steps when using the remote console.
i Press [Alt] + [z] key and hold [Alt] key down.
ii Press either [F1] or [F2] key solely to switch the window.
iii Press [Alt] + [z] key and release [Alt] key.

```
(Hint: Press Ctrl + F2 to go to the Login screen.) (*1)

xxxxxxxx
xxxxxxxxxxxxxxxxxxxxxxxxxxxxxx
```

*1: “Hint: Press Alt + F2 to go to the Login screen.” is displayed depending on the OS version.

Figure B.1.4-11 Console window 2

Copyright © 2011, 2014, Hitachi, Ltd.

CONTENTS

B.2 BIOS Setting

B.2.1 BIOS Version Checking Procedure
B.2.2 BMC Firmware Version Checking Procedure
B.2.3 BOOT Priority Order
B.2.4 Set the Time in BIOS
B.2.5 BMC Setting Procedure
B.2.6 RAID Controller Setting
B.2.7 Confirmation of CPU Virtualization Support Mechanism
B.2.8 Virtual Drive Consistency Checking Procedure
B.2.9 Other Setting/Confirmation Items

Copyright © 2011, Hitachi, Ltd.

This page is for editorial purpose only.

Copyright © 2011, Hitachi, Ltd.

B.2 BIOS Setting

B.2.1 BIOS Version Checking Procedure

NOTICE

Do not turn off the power of node while updating. Do not remove "System BIOS Update Tool" FD media or do not execute any of key operation. Any of these operation may fail the updating, and MOTHERBOARD may be broken.

NOTE:
- When requesting the system administrator for failback, failover and starting or stopping the cluster of a node, check the cluster status of the node with referring to "Maintenance Tool '2.2 Displaying the Cluster Status (clstatus)' (MNTT 02-0040)".
  After completing the operation by the system administrator, confirm the cluster status of the node with "Maintenance Tool '2.2 Displaying the Cluster Status (clstatus)' (MNTT 02-0040)". However, when the system administrator is absent, the maintenance personnel should contact to system administrator and get the permission from him/her to execute the above operation. For the execution procedure, refer to "Maintenance Tool '3.1 Failover and Node Termination to Execute the OS stop or the OS reboot' (MNTT 03-0000)".
- Open the remote console window, and then execute the procedure (1).
  For the remote console connection, refer to 'B.1.3 Connection Confirmation of the Remote Console'.

(1) Refer to "Maintenance Tool '2.2 Displaying the Cluster Status (clstatus)' (MNTT 02-0040)", and check whether the resource groups are running on the node where the BIOS version is to be confirmed. For the confirmation of the resource group activation, refer to "Maintenance Tool '2.2 Displaying the Cluster Status (clstatus)' (MNTT 02-0040)".
When the resource groups are running, request the system administrator to perform failover the resource groups to the other node to be confirmed the BIOS version to the other node, and to change the "Node Status" to "INACTIVE".
For the reference place in User's Guide describing the details about stopping a node, refer to "General 'Reference Place in User's Guide for Operating Procedures Table 4 'Stopping and starting a node'' (GENE 00-0040)", and for the reference place in User's Guide describing the details about failover/failback of a resource group, refer to "General 'Reference Place in User's Guide for Operating Procedures Table 4 'Changing the execution node of a resource group'' (GENE 00-0040)".
However, when the system administrator is absent, the maintenance personnel should contact to system administrator and get the permission from him/her to execute the above operation. For the execution procedure, refer to "Maintenance Tool '3.1 Failover and Node Termination to Execute the OS stop or the OS reboot' (MNTT 03-0000)".

Copyright © 2011, 2012, Hitachi, Ltd.

(2) Refer to "Installation '2.1 Procedure for Turning on and off the Power' (INST 02-0000)", and then execute the termination of the node.

(3) Connect the USB FDD to the node.
For how to connect the USB FDD, refer to "Hitachi Advance Server8000/RS220xK Maintenance Manual".

(4) Start the OS of the node with referring to "Installation '2.1 Procedure for Turning on and off the Power' (INST 02-0000)".
If "Press <F2> to enter SETUP" is shown on the lower left of the console window during the OS of the node is starting, press [F2] key.
If [F2] key could not be pressed, reboot the OS of the node and execute the operation from the step (4) again.

Copyright © 2011, Hitachi, Ltd.

(5) The main menu window is displayed as shown in Figure B.2.1-1.
Select [System Management], and press [Enter] key.

```
Phoenix Secure Core(tm) Setup Utility
Main        Advanced        Security        Server        Boot        Exit

                                                    Item Specific Help
  System Time:                  [HH:MM:SS]
  System Date:                  [MM/DD/YYYY]        <Tab>, <Shift-Tab>, or
                                                    <Enter>selects field.
► SATA Port 1                   [CD-ROM]

► System Management
► Advanced Processor Options

F1   Help  ↑↓  Select Item   -/+   Change Values   F9   Setup Defaults
ESC  Exit  ←→  Select Menu   Enter Select ► Sub-Menu F10  Save and Exit
```

Figure B.2.1-1 Main Menu window

NOTE: For the detailed operation method of BIOS Setup Utility, refer to “Hitachi Advance Server8000/RS220xK Maintenance Manual”.

Copyright © 2011, 2012, Hitachi, Ltd.

(6) The System Management window is displayed as shown in Figure B.2.1-2.
Check if the version displayed on [BIOS Version:] is the version that requires to update or not.
For the version confirmation, execute with reference to Version Management table (Web).
If the updating is necessary for the firmware, select [Exit] and proceed to step (7).
If the updating is not necessary for the firmware, return to the caller of the firmware update procedures and execute the rest of the operations.

Phoenix Secure Core(tm) Setup Utility

Main

System Management		Item Specific Help
BIOS Version:	xxxxxx-xxx	All items on this menu cannot be modified in user mode. If any items require changes, please consult your system Supervisor.
BMC Firmware Version:	xx.xx	
System Product Name:	HA8000/RS220	
System Version:	xxxxxxxxxx	
System Serial No:	xxxxxxxxxxxxxxxxxxxx	
Main Board Product Name:	xxxxxxx	
Base Board Serial No:	N/A	
LAN1 MAC Address:	xx-xx-xx-xx-xx	
LAN2 MAC Address:	xx-xx-xx-xx-xx	
BMC MAC Address:	xx-xx-xx-xx-xx	
Reduced Processor:	None	

F1	Help	↑ ↓	Select Item	−/+	Change Values	F9	Setup Defaults
ESC	Exit	←→	Select Menu	Enter	Select ▶ Sub-Menu	F10	Save and Exit

Figure B.2.1-2 System Management window

(7) Insert the [HA8000/RS210, RS220 (7TTSHE), TS20 (7TCSE) FW/SDR/FRU UPDATE TOOL] into the DVD ROM drive of the node.

Copyright © 2011, Hitachi, Ltd.

(8) The Termination menu window is displayed as shown in Figure B.2.1-3.
Select [Exit Discharging Changes] and press [Enter] key.

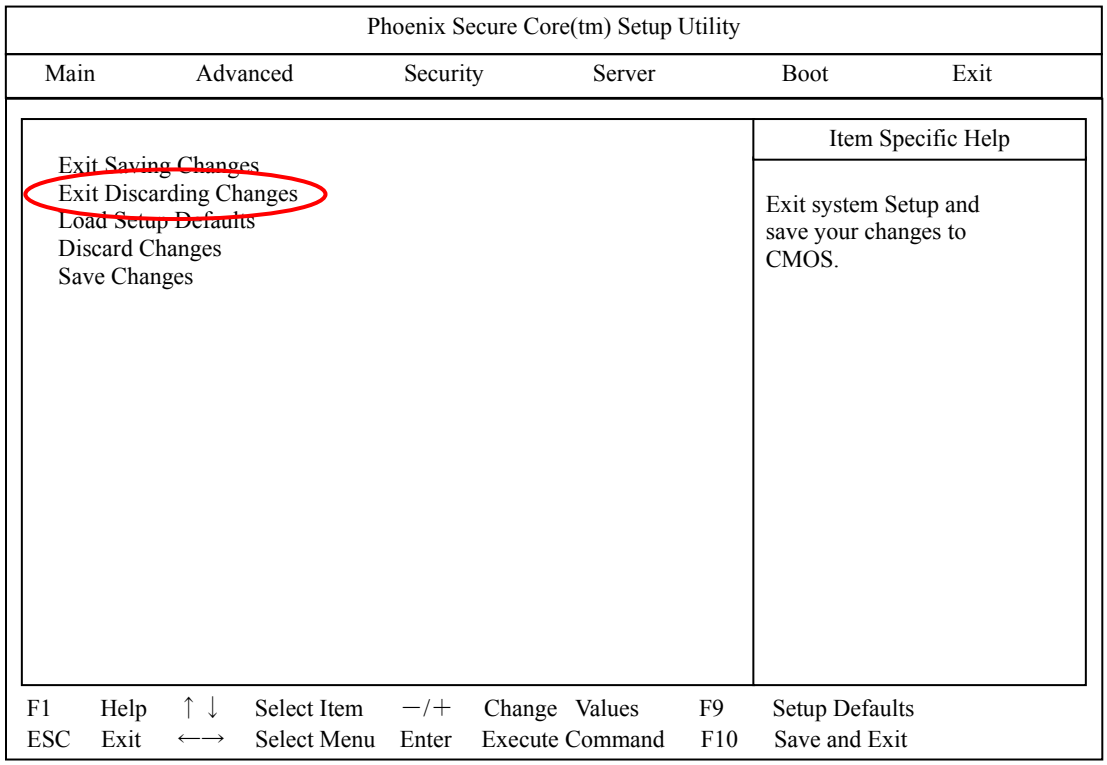


Figure B.2.1-3 Termination Menu window

Copyright © 2011, Hitachi, Ltd.

(9) When the CD boot is completed, the prompt window 1 is displayed as shown in Figure B.2.1-4.
Press [2] key.

```
1. HATP & SCSI Device Load for Ultra 320.
2. Return to DOS Prompt Mode.
3. Return to DOS Prompt Mode with RAMDISK.
4. Return to DOS Prompt Mode with CD-ROM Support.
5. Maintenance Utility Mode with RAMDISK.
6. RS440 BIOS Check Mode.
7. After xJ Model HATP & SCSI Device Load for Ultra 320.
8. After xJ Model Return to Dos Prompt Mode with RAMDISK.
9. After xJ Model Maintenance Utility Mode with RAMDISK.
0. After xK RS440 BIOS Check Mode.
```

Figure B.2.1-4 Prompt window 1

(10) Insert the [HA8000/RS210,RS220(7TTSHE),TS20(7TCSE)Standard model System BIOS Update Tool] into the USB FDD.

(11) The prompt window is displayed as shown in Figure B.2.1-5.
Input “a:” as shown in the following window, and then press [Enter] key.

```
C:\>a:
```

Figure B.2.1-5 DOC Prompt window 1

Copyright © 2011, Hitachi, Ltd.

(12) When A drive is displayed, input “biosup” as shown in the following window, and then press [Enter] key.

```
A:\> biosup
```

Figure B.2.1-6 DOC Prompt window 2

NOTE:
- Updating may take about 1 minute and 30 seconds.
- Do not turn off the power of node while updating. Do not remove “System BIOS Update Tool” FD media or do not execute any of key operation. Any of these operation may fail the updating, and MOTHERBOARD may be broken.

(13) When the updating is successfully completed, the following message is displayed and it returns to the DOS prompt window.

```
Updated Successfully.

A:\>
```

Figure B.2.1-7 DOC prompt window 3

(14) Remove the [HA8000/RS210, RS220 (7TTSHE), TS20 (7TCSE) FW/SDR/FRU UPDATE TOOL] from the DVD ROM drive of the node.

(15) Refer to “Installation ‘2.1 Procedure for Turning on and off the Power’ (INST 02-0000)”, and stop the node.

(16) Remove the FD of “System BIOS Update Tool” from FDD, and remove USB FDD from the node.
For how to remove the FD from the FDD, refer to “Hitachi Advance Server8000/RS220xK Maintenance Manual”.

(17) Press the Power lamp switch and turn the power of the node.
Refer to “Installation ‘2.1 Procedure for Turning on and off the Power’ (INST 02-0000)” for the place of the power lamp.

(18) Return to the BIOS updating procedure and continue the processing.

Copyright © 2011, 2012, Hitachi, Ltd.

This page is for editorial purpose only.

Copyright © 2011, Hitachi, Ltd.

B.2.2 BMC Firmware Version Checking Procedure

NOTE:
- When requesting the system administrator for failback, failover and starting or stopping the cluster of a node, check the cluster status of the node with referring to "Maintenance Tool '2.2 Displaying the Cluster Status (clstatus)' (MNTT 02-0040)".
  After completing the operation by the system administrator, confirm the cluster status of the node with "Maintenance Tool '2.2 Displaying the Cluster Status (clstatus)' (MNTT 02-0040)".
  However, when the system administrator is absent, the maintenance personnel should contact to system administrator and get the permission from him/her to execute the above operation. For the execution procedure, refer to "Maintenance Tool '3.1 Failover and Node Termination to Execute the OS stop or the OS reboot' (MNTT 03-0000)".
- Open the remote console window, and then execute the procedure (1).
  For the remote console connection, refer to 'B.1.3 Connection Confirmation of the Remote Console'.

(1) Refer to "Maintenance Tool '2.2 Displaying the Cluster Status (clstatus)' (MNTT 02-0040)", and check whether the resource groups are running on the node where the BMC firmware version is to be confirmed. For the confirmation of the resource group activation, refer to "Maintenance Tool '2.2 Displaying the Cluster Status (clstatus)' (MNTT 02-0040)".
When the resource groups are running, request the system administrator to perform failover the resource groups to the other node to be confirmed the BIOS version to the other node, and to change the "Node Status" to "INACTIVE".
For the reference place in User's Guide describing the details about stopping a node, refer to "General 'Reference Place in User's Guide for Operating Procedures Table 4 'Stopping and starting a node'' (GENE 00-0040)", and for the reference place in User's Guide describing the details about failover/failback of a resource group, refer to "General 'Reference Place in User's Guide for Operating Procedures Table 4 'Changing the execution node of a resource group'' (GENE 00-0040)".
However, when the system administrator is absent, the maintenance personnel should contact to system administrator and get the permission from him/her to execute the above operation. For the execution procedure, refer to "Maintenance Tool '3.1 Failover and Node Termination to Execute the OS stop or the OS reboot' (MNTT 03-0000)".

(2) Terminate the OS of the node with reference to "Installation '2.1 Procedure for Turning on and off the Power' (INST 02-0000)".

(3) Reboot the OS of the node with reference to "Installation '2.1 Procedure for Turning on and off the Power' (INST 02-0000)".

(3-1) If "Press <F2> to enter SETUP" is displayed on the lower left of the console window while the OS of the node is starting, press [F2] key.
If [F2] key could not be pressed, reboot the OS of the node and then retry the operation from the step (3) again.

Copyright © 2011, 2012, Hitachi, Ltd.

(4) The Main menu window is displayed as shown in Figure B.2.2-1.
Choose [System Management], and press [Enter] key.

```
Phoenix Secure Core(tm) Setup Utility
Main        Advanced        Security        Server        Boot        Exit

                                                    Item Specific Help
  System Time:                  [HH:MM:SS]
  System Date:                  [MM/DD/YYYY]        <Tab>, <Shift-Tab>, or
                                                    <Enter>selects field.
► SATA Port 1                   [CD-ROM]

► System Management
► Advanced Processor Options

F1   Help  ↑↓  Select Item  −/+   Change  Values     F9   Setup Defaults
ESC  Exit  ←→  Select Menu  Enter Select ► Sub-Menu   F10  Save and Exit
```

Figure B.2.2-1 Main Menu window

NOTE: For the detailed operation methods of BIOS Setup Utility, refer to “Hitachi Advance Server8000/RS220xK Maintenance Manual”.

Copyright © 2011, 2012, Hitachi, Ltd.

(5) The system management window is displayed as shown in Figure B.2.2-2.
Check if the version displayed in [BMC Firmware Version:] is the version that requires the updating or not.
Check the version with reference with the Version management table (Web).
If the updating is necessary for the firmware, choose [Exit] and proceed to step (6).
If the updating is not necessary for the firmware, return to the caller of the firmware update procedures and execute the rest of the operations.
If the newly installation or updating is not necessary for the firmware, press [Esc] key and proceed to step (5) of the 'B.2.3 BOOT Priority Order'.

```
Phoenix Secure Core(tm) Setup Utility
Main        Advanced        Security        Server        Boot        Exit

System Management                                   Item Specific Help

  BIOS Version:                    xxxxxx-xxx
  BMC Firmware Version:            xx.xx            All items on this menu
                                                    cannot be modified in
  System Product Name:             HA8000/RS220     user mode. If any
  System Version:                  xxxxxxxxxx       items require changes,
  System Serial No:                xxxxxxxxxxxxxxxxxxx please consult your
  Main Board Product Name:         xxxxxxx          system Supervisor.
  Base Board Serial No:            N/A
  LAN1 MAC Address:                xx-xx-xx-xx-xx
  LAN2 MAC Address:                xx-xx-xx-xx-xx
  BMC MAC Address:                 xx-xx-xx-xx-xx
  Reduced Processor:               None

F1   Help  ↑↓  Select Item  -/+   Change Values   F9   Setup Defaults
ESC  Exit  ←→  Select Menu  Enter Select ► Sub-Menu F10  Save and Exit
```

Figure B.2.2-2 System Management window

Copyright © 2011, Hitachi, Ltd.

(6) The exit menu window is displayed as shown in Figure B.2.2-3.
Choose [Exit Discarding Changes] and press [Enter] key.

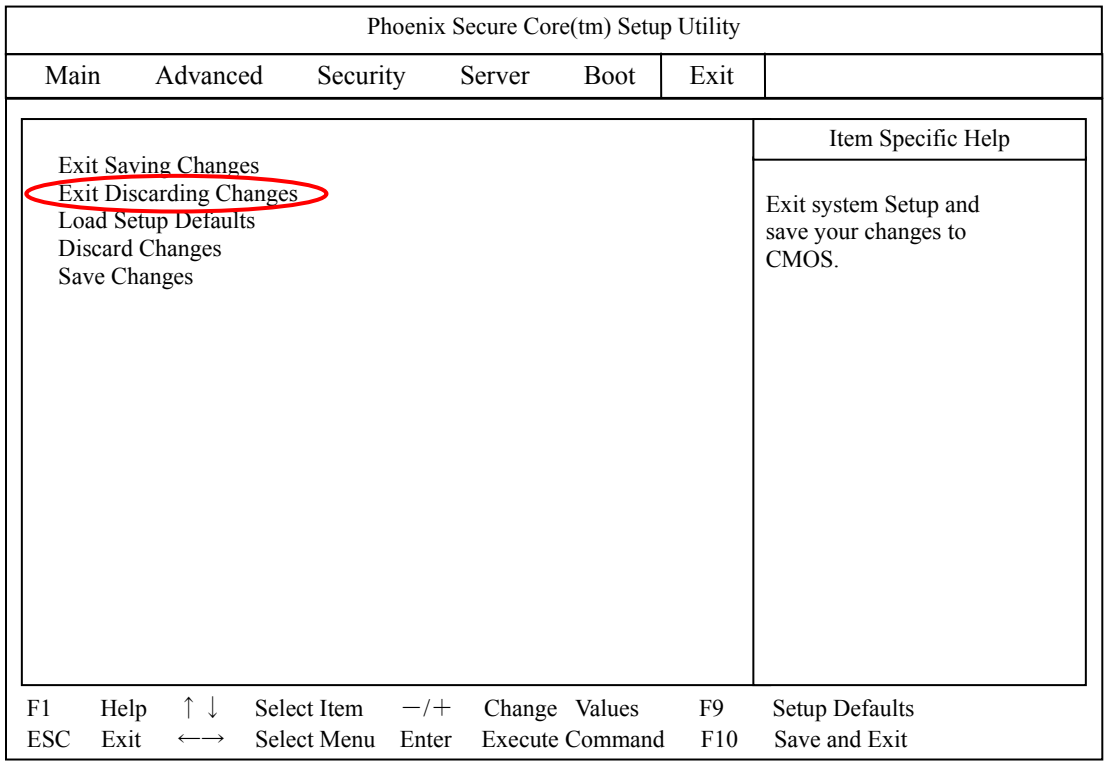


Figure B.2.2-3 Exit Menu Window

(7) Change the IP address of the maintenance PC to the IP address that belongs to the same network segment with the BMC port, and connect directory the LAN cable of the maintenance PC to the BMC port to be executed updating.

The “IP address/ Subnet mask” of the BMC port at the time of factory shipment is “192.168.100.100/255.255.255.0”.
If the IP address is other than the above, confirm the value with the system administrator.

(8) Inset the CDROM that has the firmware image file of BMC to be updated the maintenance PC.

(9) Start up the Internet Explorer from the maintenance PC.
Click [Start]-[Program]-[Internet Explorer].

(10) Input the following address in the address bar on the Internet Explorer.
“http://<IP address of the BMC to update>”

Copyright © 2011, 2013, Hitachi, Ltd.

(11) Make sure that the BMC login window is displayed.

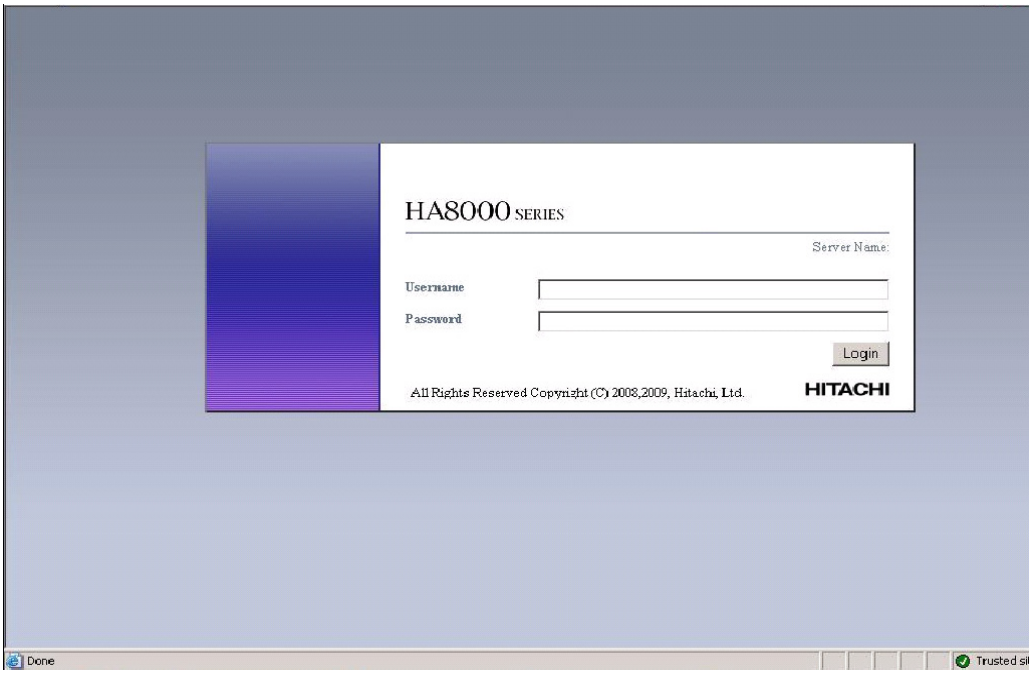


Figure B.2.2-4 BMC Login window 1

(12) Enter “ceconsl” in the [Username], and “cepasswd” in the [Password].
After the input, click [Login].

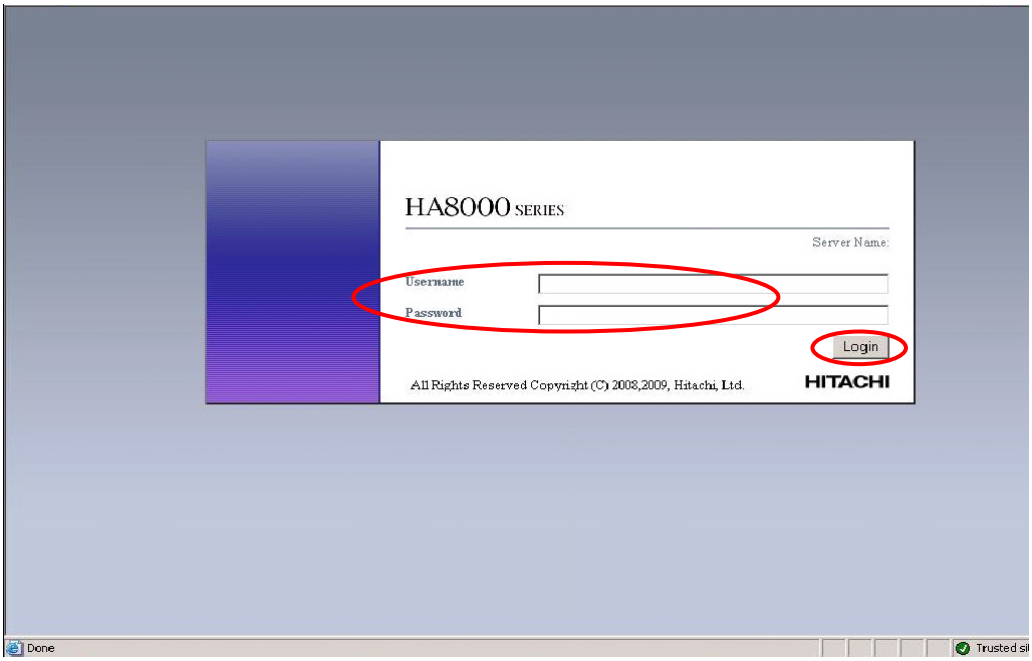


Figure B.2.2-5 BMC Login window 2

Copyright © 2011, 2014, Hitachi, Ltd.

(13) Server Information window is displayed as shown in Figure B.2.2-6.
Click [Maintenance].

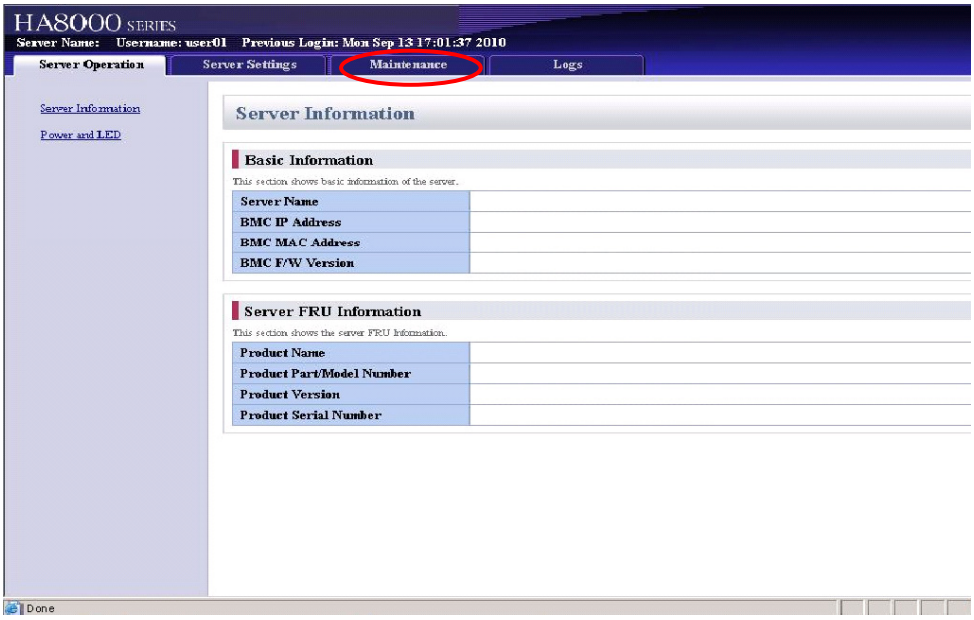


Figure B.2.2-6 Server Information window

(14) Select [BMC Firmware Management] from the tree menu in the left.
BMC Firmware Management window 1 is displayed as shown in Figure B.2.2-7.
Click [Browse] button, and select the target firmware image file to be updated that is stored in the step (8), and then click [Update BMC Firmware].

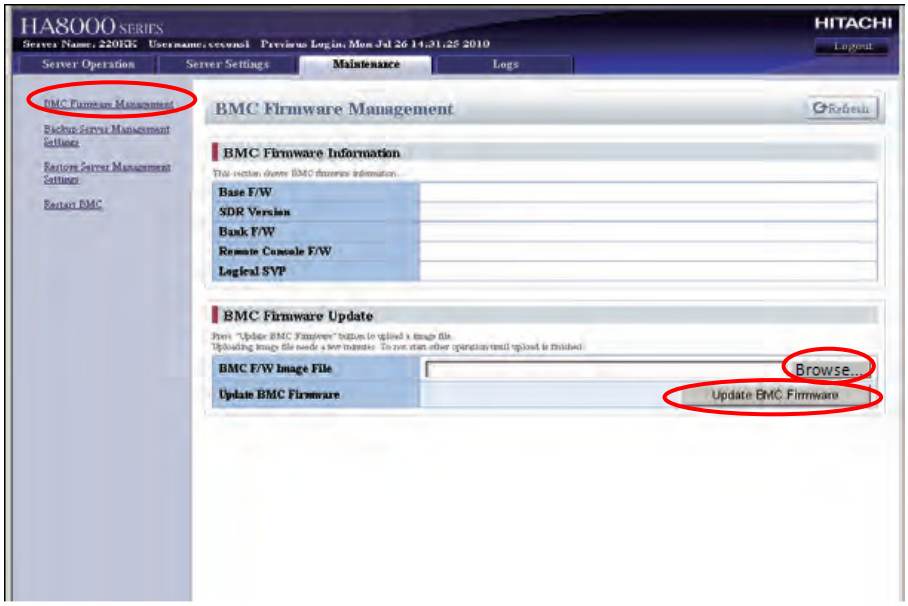


Figure B.2.2-7 BMC Firmware Management window 1

Copyright © 2011, 2015, Hitachi, Ltd.

(15) BMC Firmware Management window 2 is displayed as shown in Figure B.2.2-8.
Check if the content of BMC firmware updating has the same version with the Version Management Table (Web).
If the updated contents are the same, click [Confirm].
If the updated content is different, click [back] and execute from the step (14) again.
If the file stored in the maintenance PC is incorrect, execute from step (8) again.

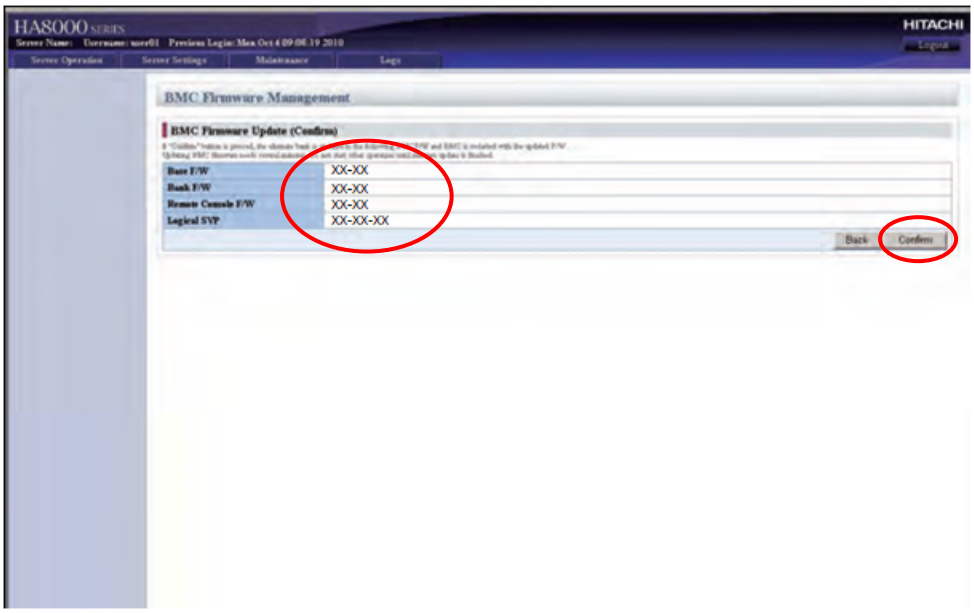


Figure B.2.2-8 BMC Firmware Management window 2

Clicking [Confirm] executes the updating of the BMC firmware image file.

(16) When the updating is completed, the Logout window is displayed as shown in Figure B.2.2-9.
Close the Internet Explorer because the BMC is rebooted automatically.

Figure B.2.2-9 Logout window

Copyright © 2011, 2015, Hitachi, Ltd.

(17) SERVICE lamp switch of the node blinks on and off for about 30 seconds.
Wait until the blinking of SERVICE lamp switch stops, and then stop the node.
For the termination of the node, refer to "Installation '2.1 Procedure for Turning on and off the Power' (INST 02-0000)".

(18) Start the OS of the node with referring to "Installation '2.1 Procedure for Turning on and off the Power' (INST 02-0000)".
If "Press <F2> to enter SETUP" is shown on the lower left of the console window during the OS of the node is starting, press [F2] key.
If [F2] key could not be pressed, reboot the node by pressing [Ctrl]+[Alt]+[Del] key and execute the operation from the step (3) again.

(19) The Main Menu window is displayed as shown in Figure B.2.2-10.
Select [System Management] and press [Enter] key.

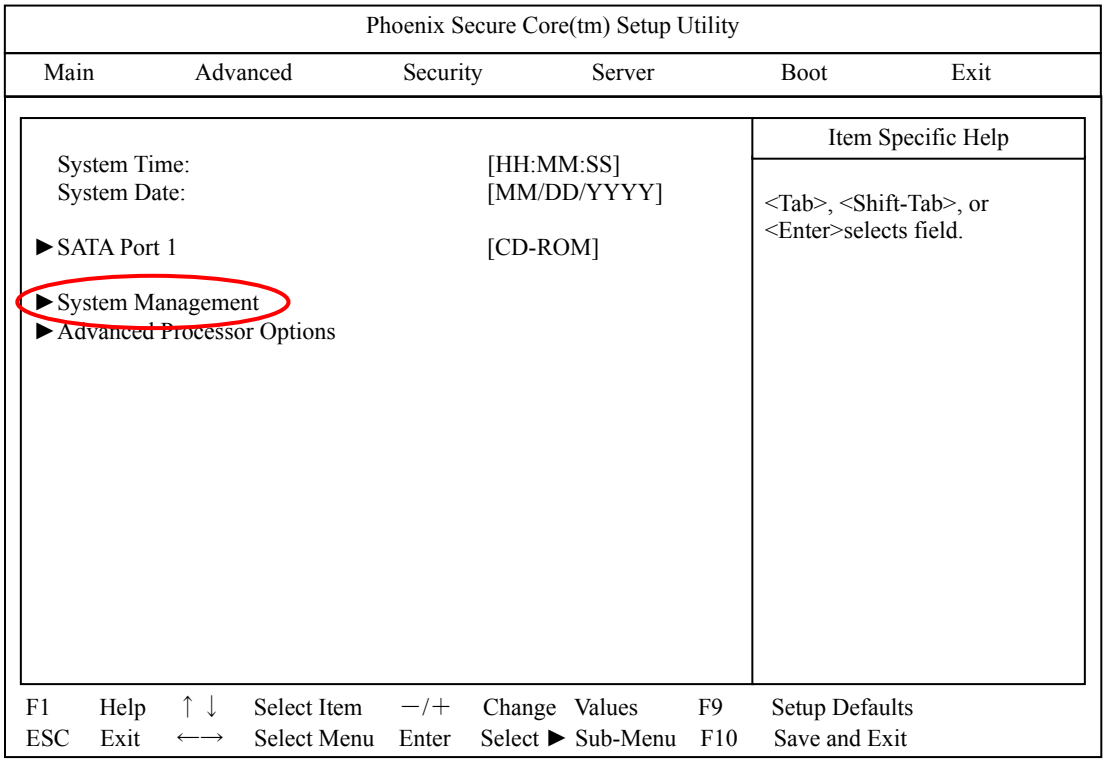


Figure B.2.2-10 Main Menu window

NOTE: For the detailed operation method of BIOS Setup Utility, refer to "Hitachi Advance Server8000/RS220xK Maintenance Manual".

Copyright © 2011, 2012, Hitachi, Ltd.

(20) The System Management window is displayed as shown in Figure B.2.2-11.
Confirm that the version displayed on [BMC Firmware Version:] is the same version with the Version Management Table (Web), and then select [Exit].

Phoenix Secure Core(tm) Setup Utility

Main

System Management		Item Specific Help
BIOS Version:	xxxxxx-xxx	All items on this menu cannot be modified in user mode. If any items require changes, please consult your system Supervisor.
BMC Firmware Version:	xx.xx	
System Product Name:	HA8000/RS220	
System Version:	xxxxxxxxxx	
System Serial No:	xxxxxxxxxxxxxxxxxxxx	
Main Board Product Name:	xxxxxxx	
Base Board Serial No:	N/A	
LAN1 MAC Address:	xx-xx-xx-xx-xx	
LAN2 MAC Address:	xx-xx-xx-xx-xx	
BMC MAC Address:	xx-xx-xx-xx-xx	
Reduced Processor:	None	

F1	Help	↑ ↓	Select Item	−/+	Change Values	F9	Setup Defaults
ESC	Exit	←→	Select Menu	Enter	Select ► Sub-Menu	F10	Save and Exit

Figure B.2.2-11 System Management window

Copyright © 2011, Hitachi, Ltd.

(21) The Termination menu window is displayed as shown in Figure B.2.2-12.
Select [Exit Discharging Changes] and press [Enter] key.

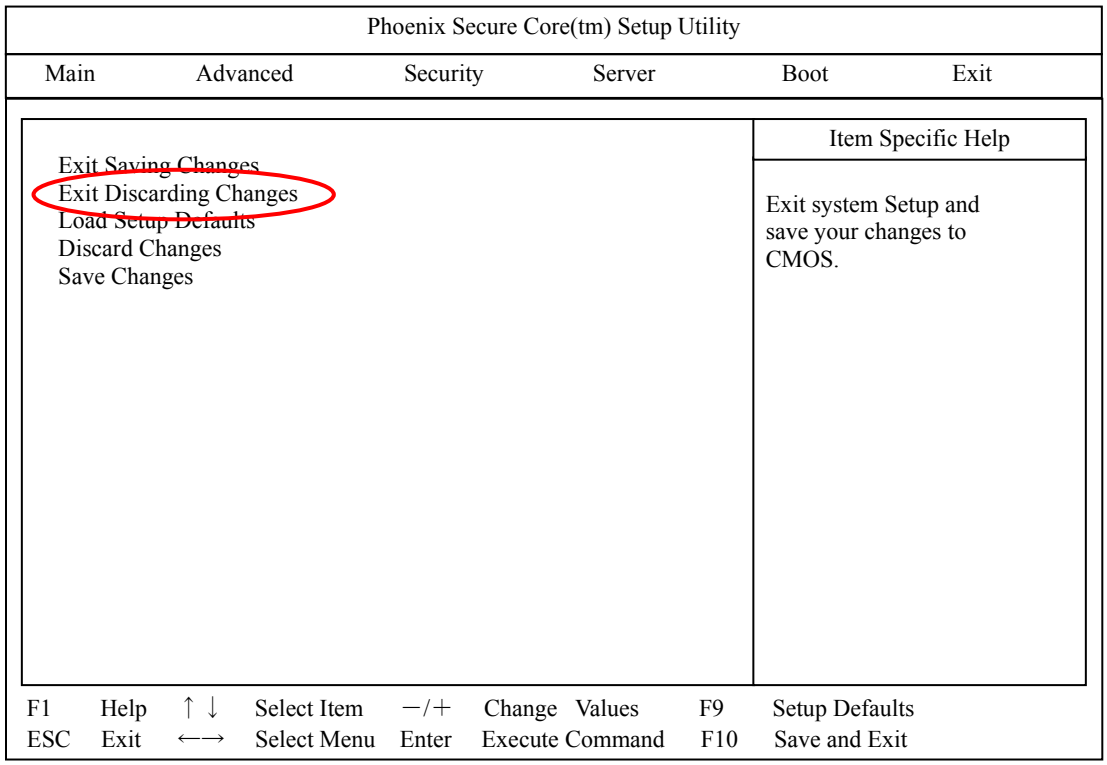


Figure B.2.2-12 Termination Menu window

(22) Return to the BMC updating procedure and continue the processing.

Copyright © 2011, Hitachi, Ltd.

B.2.3 BOOT Priority Order

NOTE: Open the remote console window, and then execute the procedure (1).
For the remote console connection, refer to ‘B.1.3 Connection Confirmation of the Remote Console’.

(1) Stop the OS of the node with referring to “Installation ‘2.1 Procedure for Turning on and off the Power’ (INST 02-0000)”. If the Power lamp is turned off, execute the procedure step (2). When the main menu window is already displayed, proceed to step (3).

(2) Start the OS of the node with referring to “Installation ‘2.1 Procedure for Turning on and off the Power’ (INST 02-0000)”.

(3) If “Press <F2> to enter SETUP” is displayed on the lower left of the console window while the OS of the node is starting up, press [F2] key.
If [F2] key cannot be pressed, execute from the step (1) again.

Copyright © 2011, 2015, Hitachi, Ltd.

(4) The main menu window is displayed as shown in Figure B.2.3-1.
Select [Boot].

```
Phoenix Secure Core(tm) Setup Utility
Main    Advanced    Security    Server    Boot    Exit

System Time:                    [HH:MM:SS]          Item Specific Help
System Date:                    [MM/DD/YYYY]
                                                    <Tab>, <Shift-Tab>, or
►SATA Port 1                    [CD-ROM]            <Enter>selects field.

►System Management
►Advanced Processor Options

F1   Help  ↑↓  Select Item  -/+   Change Values   F9   Setup Defaults
ESC  Exit  ←→  Select Menu  Enter Select ► Sub-Menu F10  Save and Exit
```

Figure B.2.3-1 Main Menu window

NOTE: For the detailed operation method of BIOS Setup Utility, refer to “Hitachi Advance Server8000/RS220xK Maintenance Manual”.

Copyright © 2011, 2015, Hitachi, Ltd.

(5) The Boot menu window is displayed as shown in Figure B.2.3-2.
Check that the items displayed under [Boot priority order] are listed as the order shown in Figure B.2.3-2.
The items displayed under [Excluded from boot order] indicate that the device is inactivated. If you want to activate the device, place the cursor on the device that you want to be embedded, and press “X” key.
If the display order differs, sort them by using the [+] key and the [-] key.

NOTE: When entering characters in the BIOS setup utility window, the keyboard layout is recognized as the 101 series Keyboard (QWERTY based layout).

```
Phoenix Secure Core(tm) Setup Utility
Main   Advanced   Security   Server   Boot   Exit

Boot priority order                          Item Specific Help
  1: USB FDC: xxxxxxxxxx                     Keys used to views or
  2: IDE 0: xxxxxxxxxx                       configure devices :
  3: USB CDROM:                              Up and Down arrows
  4: PCI SCSI:（Bus xx Dev xx） xxxxxxxxxx    select a device.
  5: PCI BEV:                                <+>and<->moves
  6: USB KEY:                                the device up or down.
  7:                                         <f>and<r>specifies
  8:                                         the device fixed or
Excluded from boot order:                    removable.
   : USB HDD :                               <x>exclude or include
   : Other USB:                              the device to boot.
   : PCI :                                   <Shift+1>enables or
   : Legacy Net work Card                    disables a device.
   : Bootable Add-in Cards                   <1-4>Loads default
                                             boot sequence

F1   Help  ↑↓  Select Item  -/+   Change Values   F9   Setup Defaults
ESC  Exit  ←→  Select Menu  Enter Select ▶ Sub-Menu F10  Save and Exit
```

Figure B.2.3-2 Boot Menu window

Copyright © 2011, 2015, Hitachi, Ltd.

(6) The procedure differs whether the setting was changed in step (5) or not.
If the setting has been changed, proceed to step (a).
If the setting has not been changed, proceed to step (b).

(a) Press [F10] key. Then, Figure B.2.3-3 Setup Confirmation window is displayed.
Select [Yes] and press [Enter] key.

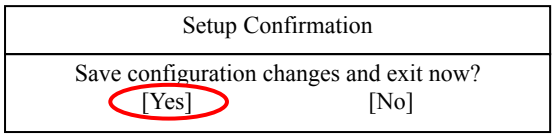


Figure B.2.3-3 Setup Confirmation window

(b) Select [Exit] in the boot menu window as shown in Figure B.2.3-2.
The exit menu window is displayed as shown in Figure B.2.3-4.
Select [Exit Discarding Changes] and press [Enter] key.
When holding down [Enter] key, node is activated automatically.

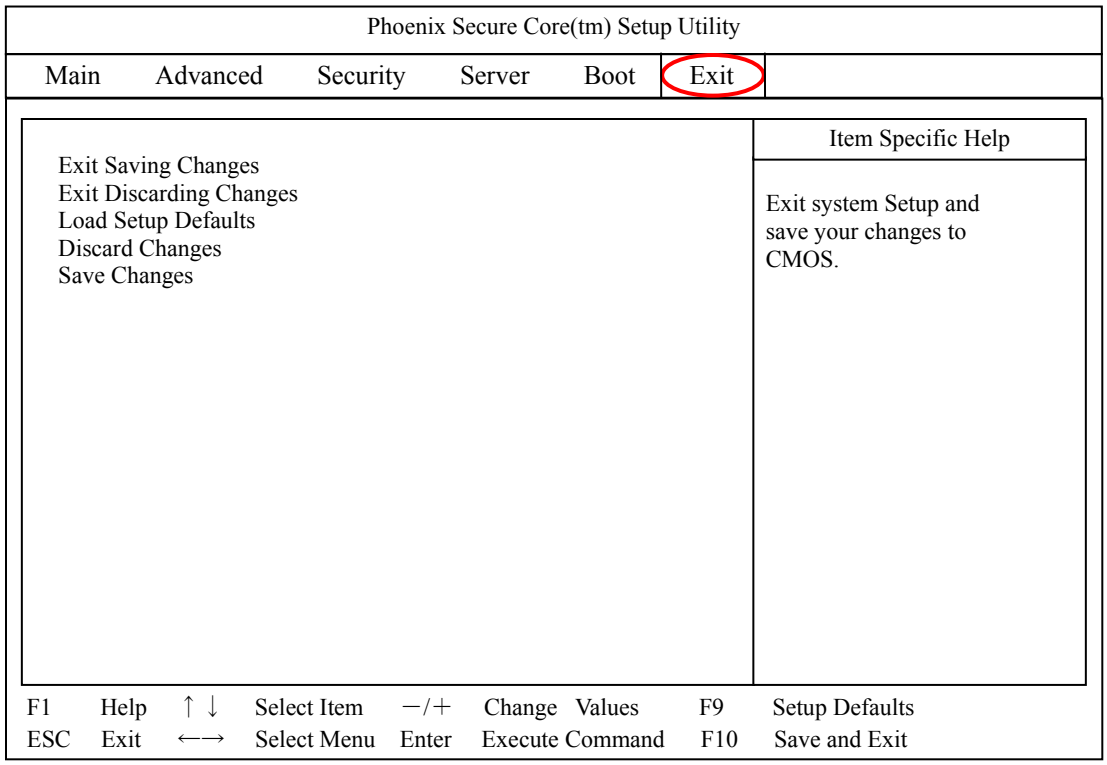


Figure B.2.3-4 Exit Menu window

(7) Return to the caller of the BOOT priority order and execute the rest of the operations.

Copyright © 2011, 2015, Hitachi, Ltd.

B.2.4 Set the Time in BIOS

Set the time in BIOS from the main menu window.

To obtain the time to enter, it is required to display "Set Up 'Figure 9.1-7 "Date and Time" window 4' (SETUP 09-0030)" or run the timeget-u command on the other side node in advance.

NOTE: The timeget-u command can be run only when the mother board is replaced.

(1) Start the node. When "Press <F2> to enter SETUP" is displayed on the lower left of the console window, press [F2] key.
If [F2] key cannot be pressed, reboot the node and then execute from step (1) again.
When the Main Menu window is already running, proceed to step (2).

(2) Select "System Time" from the Figure B.2.4-1 Main Menu Window, and then manually enter the UTC time that is obtained from/by either of the following:
The difference between the entered time and the obtained UTC time must be within 10 seconds.
- "Set Up 'Figure 9.1-7 "Date and Time" window 4' (SETUP 09-0030)"
- Running the timeget-u command on the other side node
  Refer to "Maintenance Tool '2.42 Acquisition of Time/Time Zone (timeget)' (MNTT 02-2430)" for details.

(3) Select "System Date" from the Figure B.2.4-1 Main Menu Window, and then manually enter the UTC date that is obtained by the same procedure as the step (2) above.

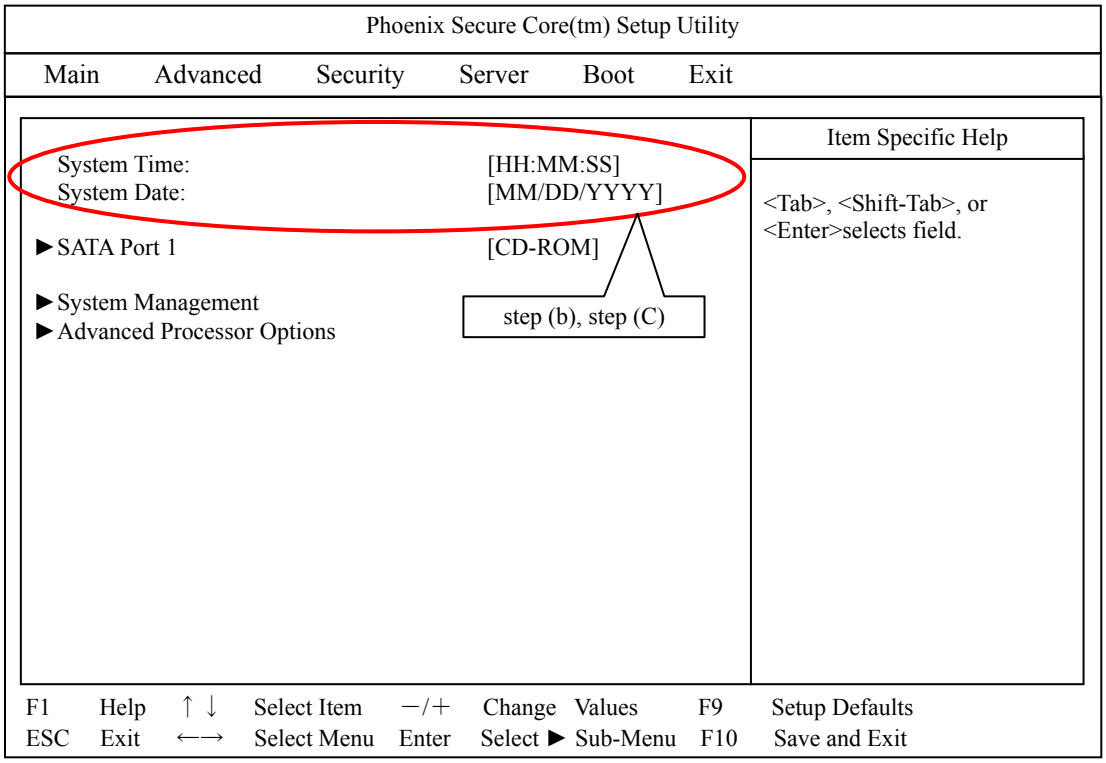


Figure B.2.4-1 Main Menu window

Copyright © 2011, 2015, Hitachi, Ltd.

(4) Press [F10] key. The setup confirmation window is displayed as shown in Figure B.2.4-2.
Select [Yes] and press [Enter] key.
Clicking [Enter] key automatically reboots the node.

Setup Confirmation
Save configuration changes and exit now? [Yes] [No]

Figure B.2.4-2 Setup Confirmation window

Copyright © 2011, 2014, Hitachi, Ltd.

B.2.5 BMC Setting Procedure

The setting procedure of BMC is unnecessary for the model: HA8000.

Return to the caller of the BMC setting procedures and execute the rest of the operations.

Copyright © 2011, Hitachi, Ltd.

B.2.6 RAID Controller Setting

The setting procedure of RAID controller is unnecessary for the model: HA8000.

Return to the caller of the RAID controller setting procedures and execute the rest of the operations.

Copyright © 2011, Hitachi, Ltd.

B.2.7 Confirmation of CPU Virtualization Support Mechanism

Verify the CPU virtualization support mechanism from the main menu window.

(a) Terminate the OS of the node with reference to "Installation '2.1 Procedure for Turning on and off the Power' (INST 02-0000)". If the node is stopped already, proceed to step (b).

(b) Reboot the OS of the node with reference to "Installation '2.1 Procedure for Turning on and off the Power' (INST 02-0000)", and if "Press <F2> to enter SETUP" is displayed on the lower left of the console window while the OS of the node is starting, press [F2] key.
If [F2] key could not be pressed, retry the operation from the procedure (a).
If the main menu is started already, proceed to step (c).

(c) The Main menu window is displayed as shown in Figure B.2.7-1.
Select [Advanced Processor Options], and press [Enter] key.

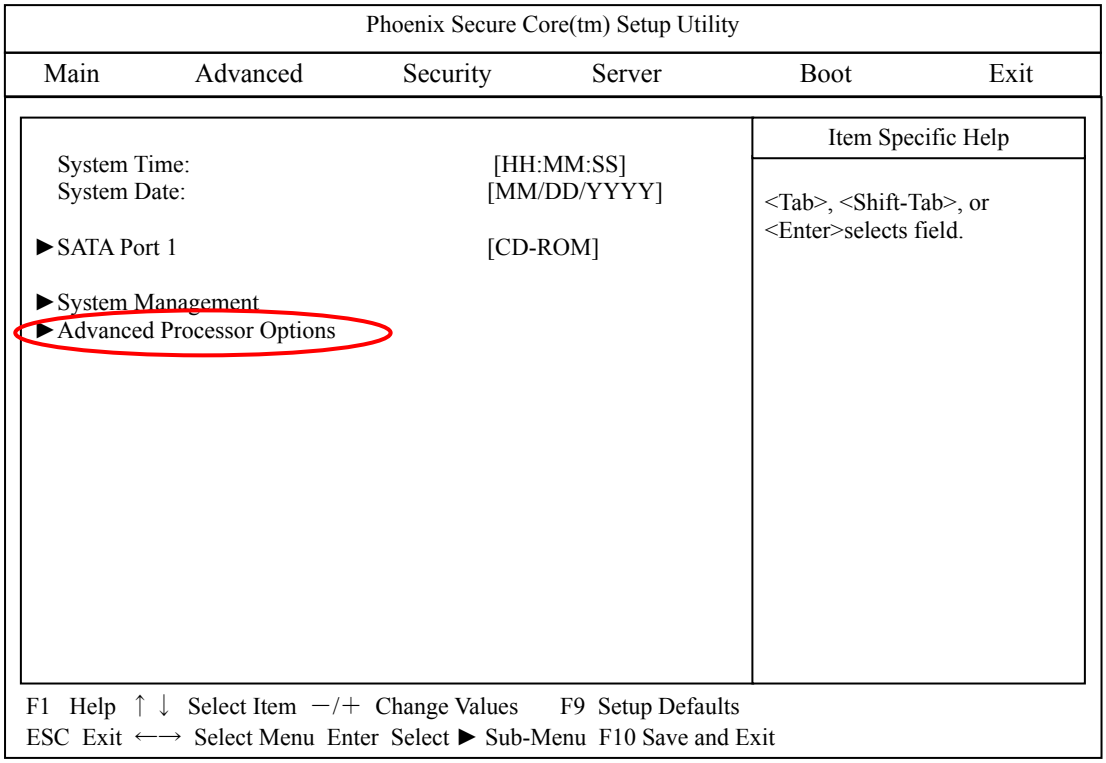


Figure B.2.7-1 Main Menu window

NOTE: For the details about the operation method of BIOS Setup Utility, refer to "Hitachi Advance Server8000/RS220xK Maintenance Manual".

Copyright © 2011, 2012, Hitachi, Ltd.

(d) Advanced Processor Options window is displayed as shown in Figure B.2.7-2.
Check that [Intel(R) Virtualization Technology] is [Enabled].
When it shows [Enabled], proceed to step (e).
When it shows [Disabled], select [Intel(R) Virtualization Technology] and change the status to [Enabled].

```
Phoenix Secure Core(tm) Setup Utility
Main

Advanced Processor Options                    Item Specific Help

  CPU Speed                          xxxx MHz
  Processor CPUID:                   xxxxxxx
  Processor L2 Cache:        xxxxkB
  Processor 1 L3 Cache:              xxxxkB
  QPI Frequency:                     x.xxx GT/s

► Nehalem CPU Power Management

  NUMA Aware                         [Enabled]
  ACPI SRAT Report                   [Enabled]

  Active Processors          [MAX. Cores]
  Intel(R) HT Technology             [Enabled]
  Performance/Wait                   [Traditional]

  Intel(R) Virtualization Technology [Enabled]
  A20M Support                       [Enabled]
  Machine Checking                   [Enabled]

  Execute Disable Bit        [Enabled]
  Hardware Prefetcher        [Enabled]
  Adjacent Cache Line Prefetch [Enabled]

  Discrete MTRR Allocation           [Disabled]

  DCU IP Prefetch                    [Enabled]
  DCU Streamer Prefetch              [Enabled]
  Data Reuse Optimization            [Enabled]

F1  Help ↑↓ Select Item −/+ Change Values    F9  Setup Defaults
ESC Exit ←→ Select Menu Enter Select ► Sub-Menu F10 Save and Exit
```

Figure B.2.7-2 Advanced Processor Options window

Copyright © 2011, 2014, Hitachi, Ltd.

(e) Procedure will be varied depending on whether the BIOS setting has been changed in step (d).
If the setting has been changed, proceed to (e-1).
If the setting has not been changed, proceed to (e-2).

(e-1) Press [F10] key. Then Figure B.2.7-3 Setup Confirmation window is displayed.
Select [Yes] and press [Enter] key.
When holding down [Enter] key, node is activated automatically.
Proceed to step (f).

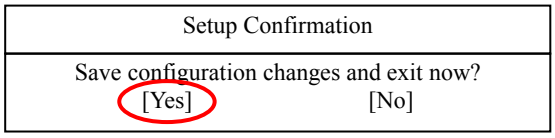


Figure B.2.7-3 Setup Confirmation window

(e-2) Select [Exit] in the main menu window as shown in Figure B.2.7-4.

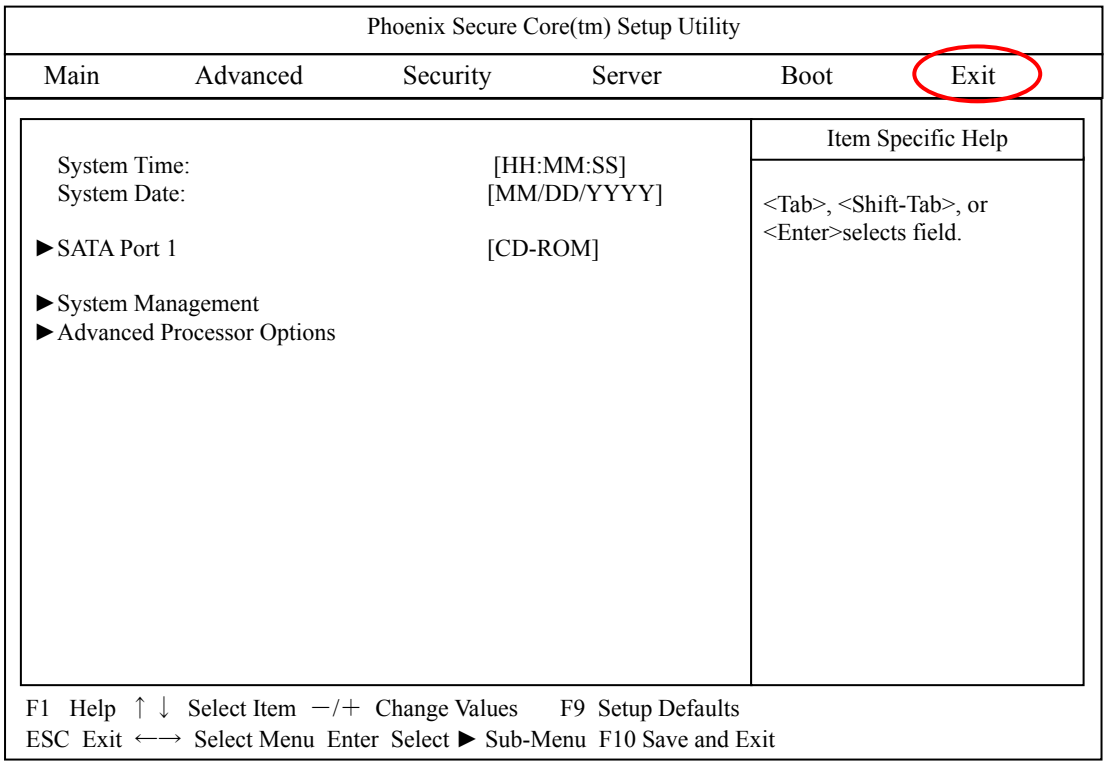


Figure B.2.7-4 Main Menu Window

Copyright © 2011, 2015, Hitachi, Ltd.

The termination menu window is displayed as shown in Figure B.2.7-5.
Select [Exit Discarding Changes] and press [Enter] key.

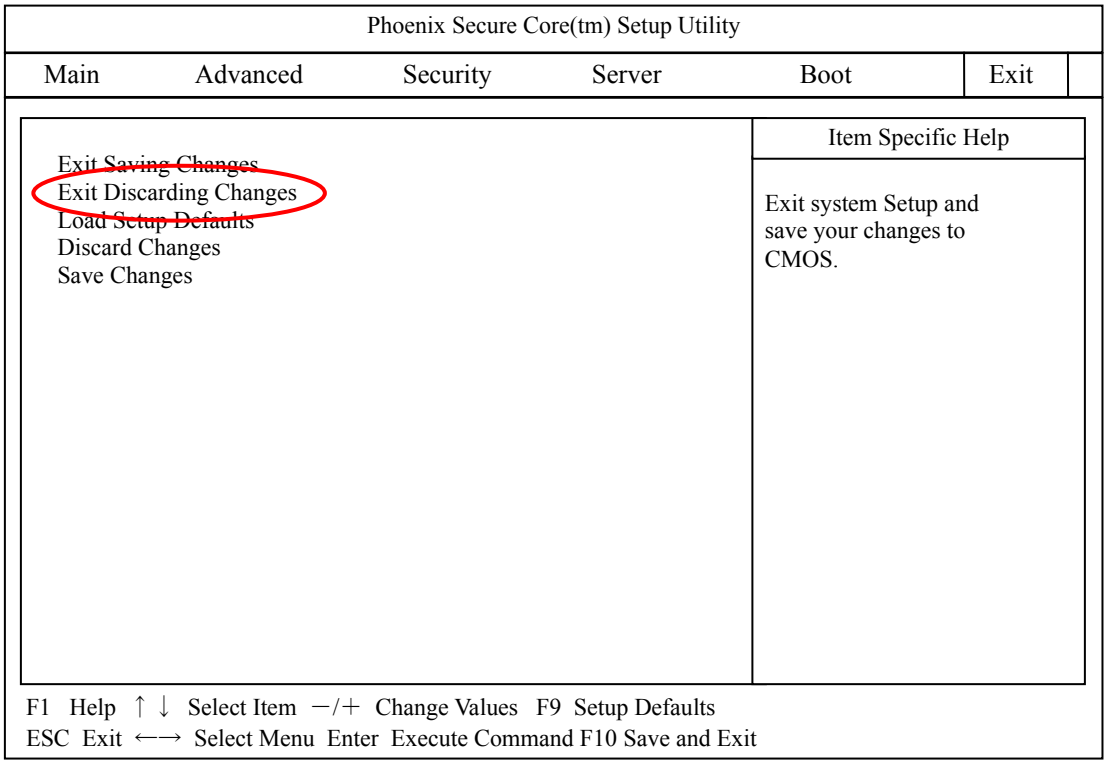


Figure B.2.7-5 Termination menu window

(f) Return to the confirmation of CPU Virtualization support mechanism and continue the processing.

Copyright © 2011, 2015, Hitachi, Ltd.

B.2.8 Virtual Drive Consistency Checking Procedure

The virtual drive consistency checking procedure is not necessary when the target model is HA8000 RS220xK.

Return to the caller of the virtual drive consistency checking procedure and execute the rest of the operations.

Copyright © 2012, Hitachi, Ltd.

B.2.9 Other Setting/Confirmation Items

There is no item to set or confirm for HA8000 RS220xK in this chapter.

Copyright © 2012, 2014, Hitachi, Ltd.

CONTENTS

B.3 Maintenance CLI

B.3.1 Displaying the Hardware Status (hwstatus)

B.3.1.1 Command line

B.3.1.2 Output format

B.3.1.3 Execution procedure

B.3.1.4 Command termination messages and action to be taken

Copyright © 2011, Hitachi, Ltd.

This page is for editorial purpose only.

Copyright © 2011, Hitachi, Ltd.

B.3 Maintenance CLI

B.3.1 Displaying the Hardware Status (hwstatus)

The hwstatus command displays the hardware status of the node.

B.3.1.1 Command line

The command line of the hwstatus command can use the following options.

hwstatus [-h]

Table B.3.1.1-1 shows the description of the options.

Table B.3.1.1-1 Command Options

No.	Option	Description	Remarks
1	-h	Displays the format of the command.	—

Copyright © 2011, Hitachi, Ltd.

B.3.1.2 Output format

The output format at the time of hwstatus command execution is shown in Figure B.3.1.2-1, and the contents of the output format are shown in Table B.3.1.2-1.

```
Output format of hwstatus

Model Information                                                                   1
 HITACHI      HA8000/RS220
SerialNumber Information                                                            2
 4230MB0-T019000015
Fan Information                                                                     3
 0            ok                    -
 1            failed                -
(Repeat for the number of cooling fan unit)
Temperature Information                                                             4
 0            ok                    reading:33_(+/-_1)_degrees_C
(Repeat for the number of temperature sensor.)
PowerSupply Information                                                             5
 0            ok                    -
 1            failed                -
Memory Information                                                                  6
 0            installed             locator:DIMM_XX,size:YYYY_MB
 1            not_installed         locator:DIMM_XX,size:-
(Repeat for the number of DIMMs)
MemoryTotal Information                                                             7
 0            -                     size: 5.5  GB(6.0  GB)
InternalHDD Information                                                             8
 0            ok                    size:XXX.XXX_GB,raid_level:RAIDX,media_error:0,predictive_failure:0
 1            failed                size:XXX.XXX_GB,raid_level:RAIDX,media_error:0,predictive_failure:0
InternalRAIDBattery Information                                                     9
 -            -                     -
BMC Information                                                                     10
 status       ok
 connection   ok
Network Interface                                                                   11
 mng0         up                    linkspeed: XXXXBase,mediatype:Copper,Management port
 hb0          down                  linkspeed: XXXXBase,mediatype:Copper,Heartbeat port
 (Repeat for the number of port names)
FC Port Information                                                                 12
 fcXXXX       up       wwpn: xxxxxxxxxxxxxxxx, linkspeed:8_Gbit
 fcXXXX       up       wwpn: xxxxxxxxxxxxxxxx, linkspeed:8_Gbit
(Repeat for the number of port names)
```

Figure B.3.1.2-1 hwstatus Output Format

Copyright © 2011, 2015, Hitachi, Ltd.

Table B.3.1.2-1 Contents of Output Format (1/3)

No.	Item	Description	Remarks
1	Model Information		
	HITACHI	Displays the name of manufacturer.	HITACHI
	HA8000/ RS220	Displays the name of a product. The product name is shown after the manufacturer.	HA8000/ RS220
2	Serial Number Information		
	XXXXXXXXXX	Displays the serial number of a model.	—
3	Fan Information		
	0, 1, •••	Displays the sequential serial numbers of cooling fan unit.	0 to 5
	ok, failed	Displays the availability of failures of cooling fan unit. (*1)	ok : Normal status failed : Abnormal status Usually everything is “ok”.
	-	Displays the vendor's unique information acquired by the hardware.	Usually displays a hyphen.
4	Temperature Information		
	0, 1, •••	Displays the sequential system thermometer of serial numbers.	0 to 6
	ok, failed	Displays the status of the system temperature. (*1)	ok : Normal status failed : Abnormal status Usually everything is “ok”.
	reading: 33_(+/-_1)_degrees_C	Displays the vendor’s unique information acquired by the hardware.	The format depends on the vendor. (*2)
5	Power Supply Information		
	0, 1	Displays the sequential serial numbers of the power supply unit.	0 to 1
	ok, failed, not_installed	Displays the availability of power supply unit failures. (*1)	ok : Normal status failed : Abnormal status not_installed : Not installed
	-	Displays the vendor’s unique information acquired by the hardware.	Usually displays a hyphen.
6	Memory Information		
	0, 1, •••	Displays the sequential serial numbers of Memories.	0 to 11
	installed, not_installed	Displays the information of DIMM. (*1)	installed : Installed not_installed : Not installed
	locator:DIMM_XX, size:YYYY_MB	Displays the vendor’s unique information acquired by the hardware.	The format depends on the vendor. (*2)
7	MemoryTotal Information		
	0	Displays the total number of Memory in numerical order.	0
	-	Displays “-”. (*9)	—
	size: xx_GB(yy_GB)	Displays the vendor’s unique information acquired by the hardware.	Displays the total sum of Memory in GB. By the configuration of the system, the total number of memory may display smaller than the installed memory that is displayed in the parentheses. (*2)

Copyright © 2011, 2014, Hitachi, Ltd.

Table B.3.1.2-1 Contents of Output Format (2/3)

No.	Item	Description	Remarks
8	Internal HDD Information		
	0, 1, ...	Displays the sequential serial numbers of Internal HDD.	0 to 1 : In the cluster configuration 0 to 5 : In the single node configuration
	ok, rebuild, failed, not_supported	Displays the embedded HDD status. (*1)	ok : Normal status rebuild : RAID is being rebuilt failed : A hardware failure was detected in the disk. Some disks have failures or do not exist. not_supported : information cannot be get due to no installation of MegaCLI.
	size:XXX.XXX_GB, raid_level:RAIDX, media_error:X,predictive_failure:X	Displays the vendor's unique information acquired by the hardware.	The format is vendor dependent. (*2) media_error:X is "1" in the case that the media error count has exceeded the threshold value. And X is "0" in the case that the media error count has been under the threshold value. A hyphen is displayed in case of an information acquisition failure. predictive_failure:X is "1" in the case that S.M.A.R.T. warnings has exceeded the threshold. And X is "0" in the case that S.M.A.R.T. warnings has been under the threshold. A hyphen is displayed in case of an information acquisition failure. (*11)
9	InternalRAIDBattery Information		
	0, 1,…	Displays the sequential serial number of Internal RAIDBattery.	In the either case shown below, displays "-". • In the cluster configuration. • In the single node configuration connected to the disk array subsystem. • Acquisition of the information has failed. • OS version 4.1.2-XX or later (because the RAID battery charge status is not monitored)
	ok, failed, charging, not_supported	Displays the charge status of the RAID battery. (*1)	
	state_of_charge:XX_%	Displays the vendor's unique information acquired by the hardware.	
10	BMC Information		
	status ok, status Unknown!	Displays this side node BMC status.	ok : Normal status Unknown! : Information acquisition of BMC fails
	connection ok, connection failed, connection none	Displays the other side node BMC connection status.	(*6) ok : Normal status failed : Communication with BMC of the other side node fails. none : Cluster is not built

Copyright © 2011, 2015, Hitachi, Ltd.

Table B.3.1.2-1 Contents of Output Format (3/3)

No.	Item	Description	Remarks
11	Network Interface		
	mng0, hb0, pm0, pm1, ethX, •••	Displays the port name. (*3) (*4) (*8)	mng0 : Management port hb0 : Heartbeat port (*6) pmX : Maintenance port ethX : Data port * X indicates an integer more than or equal to 0. Example: pm0, eth1
	up, down	Displays the port status. (*3) (*4)	up : LinkUp down : LinkDown * The port not connecting the cable displays “down”. (*5)
	linkspeed: XXXXBase, linkspeed: Unknown!	Displays the link speed. (*4)	10Base : 10Mbps 100Base : 100Mbps 1000Base : 1Gbps Unknown! : Link speed is unknown
	mediatype:Copper	Displays the media type. (*3) (*4)	Copper : Copper wire
	Management port, Heartbeat port, Private maintenance port	Displays the use. (*4)	Management port : In case the port name is “mng0” Heartbeat port : In case the port name is “hb0” Private Maintenance port : In case the port name is “pm0, pm1” * The use is not displayed for other ports.
12	FC Port Information (*10)		
	fcXXXX, …	Displays the Fibre Channel port name in ascending order. (*1)	X represents an integer greater than or equal to 0. (Hexadecimal)
	up, down	Displays the port status. (*1)	up : LinkUp down : LinkDown
	wwpn: xxxxxxxxxxxxxxxx	Displays the host port WWN. (*1)	—
	linkspeed:8_Gbit	Displays the link speed. (*1)	1_Gbit : 1Gbps 2_Gblt : 2Gbps 4_Gbit : 4Gbps 8_Gbit : 8Gbps 10_Gbit : 10Gbps 16_Gbit : 16Gbps Unknown! : Displayed during LinkDown or for link speeds that are not supported

Copyright © 2012, 2014, Hitachi, Ltd.

*1: In case of an information acquisition failure, a hyphen is displayed. Note that, even in case of an information acquisition failure, the information already acquired is displayed.
*2: When the vendor's unique information does not exist, a hyphen is displayed.
*3: When the acquisition of the statuses of all pots failed, the Network Interface information is displayed in only one row. In this case, a hyphen is displayed for the port name, the port status, and the media type.
*4: When the acquisition of the status in units of ports fails, the information of the port which failed the acquisition is not displayed.
*5: Unused (unset) data port also displays "down". In this case, check if "(Not used)" is displayed just after the name of interface, by using iflist -v command. To execute this operation, refer to "Maintenance Tool '2.4 Displaying the Network Status (iflist)' (MNTT 02-0200)".
*6: Not displayed in the case of single node configuration.
*7: The number differs depending on the configuration.
*8: In case of checking the network setting of hb0, specify the "-v" option for the clstatus command and execute. For details, refer to "Maintenance Tool '2.2 Displaying the Cluster Status (clstatus)' (MNTT 02-0040)".
*9: Nothing is shown on the OS version 3.0.0-XX or later. For checking the OS version, refer to "Maintenance Tool '2.34 Displaying the Version of the OS (versionlist)' (MNTT 02-2060)".
*10: Nothing is shown on the OS version 5.1.0-XX or earlier. For checking the OS version, refer to "Maintenance Tool '2.34 Displaying the Version of the OS (versionlist)' (MNTT 02-2060)".
*11: "media_error" and "predictive_failure" is displayed on the OS version 5.2.0-XX or later. For checking the OS version, refer to "Maintenance Tool '2.34 Displaying the Version of the OS (versionlist)' (MNTT 02-2060)".

Copyright © 2014, 2015, Hitachi, Ltd.

B.3.1.3 Execution procedure

This subsection describes the procedure for executing the hwstatus command.

(1) Log in to the execution node via ssh from the maintenance PC usually. For the login method, refer to "Maintenance Tool '1.3 Procedures for Operating Commands' (MNTT 01-0200)".

(2) Execute the hwstatus command by each node. Figure B.3.1.3-1 shows display examples at the time of hwstatus execution.
If the hwstatus command terminated abnormally, the hardware status is not displayed, and the message ID is displayed. In this case, refer to 'B.3.1.4 Command termination messages and action to be taken', and take actions.

Copyright © 2011, Hitachi, Ltd.

```
$ sudo hwstatus
Model Information
 HITACHI      HA8000/RS220
SerialNumber Information
 4230MB0-T019000015
Fan Information
 0            ok             -
 1            ok             -
 2            ok             -
 3            ok             -
 4            ok             -
 5            ok             -
Temperature Information
 0            ok             reading:43_(+/-_0.500)_degrees_C
PowerSupply Information
 0            ok             -
 1            ok             -
Memory Information
0             not_installed  locator:P1C0D1,size:-
 1            installed      locator:P1C0D0,size:2048_MB
 2            not_installed  locator:P1C1D1,size:-
 3            installed      locator:P1C1D0,size:2048_MB
 4            not_installed  locator:P1C2D1,size:-
 5            installed      locator:P1C2D0,size:2048_MB
 6            not_installed  locator:P0C0D1,size:-
 7            installed      locator:P0C0D0,size:2048_MB
 8            not_installed  locator:P0C1D1,size:-
 9            installed      locator:P0C1D0,size:2048_MB
 10           not_installed  locator:P0C2D1,size:-
 11           installed      locator:P0C2D0,size:2048_MB
MemoryTotal Information
 0            -              size: 11.5_GB(12.0_GB)
InternalHDD Information
 0            ok             size: 278.875_GB,raid_level:RAID1,media_error:0,predictive_failure:0
 1            ok             size: 278.875_GB,raid_level:RAID1,media_error:0,predictive_failure:0
InternalRAIDBattery Information
 -            -              -
BMC Information
 status       ok
 connection   ok
Network Interface
 mng0         up             linkspeed: 1000Base,mediatype:Copper,Management port
 hb0          up             linkspeed: 1000Base,mediatype:Copper,Heartbeat port
 eth16        up             linkspeed: 1000Base,mediatype:Copper
 eth17        down           linkspeed: Unknown!,mediatype:Copper
 eth18        down           linkspeed: Unknown!,mediatype:Copper
 eth19        down           linkspeed: Unknown!,mediatype:Copper
 pm0          up             linkspeed: 1000Base,mediatype:Copper,Private maintenance port
 pm1          down           linkspeed: Unknown!,mediatype:Copper,Private maintenance port
```

Figure B.3.1.3-1 Display Examples at the time of hwstatus Execution

Copyright © 2011, 2015, Hitachi, Ltd.

B.3.1.4 Command termination messages and action to be taken

A message may be displayed when the hwstatus command is executed. Actions to be taken against messages are described in Table B.3.1.4-1 “Message IDs and Actions to be Taken”.

Table B.3.1.4-1 Message IDs and Actions to be Taken

No.	Message ID	Message	Description	Action
1	KAQM14131-E	A syntax error exists in the parameter (<*parameter*>).	The parameter has an error.	Specify the correct parameter, and execute it again.
2	KAQM14134-E	An error occurred in the shared processing of commands. (Error = <*error*>)	An error occurred in the common processing of the command.	Collect the OS log, and send it to the support center. To collect the OS log, refer to “Maintenance Tool ‘2.19 Collecting Logs (oslogget)’ (MNTT 02-1300)”.
3	KAQM14136-I	Usage: <*command-syntax*>	The command format is output.	Not required to be corresponding. Displayed when the –h option is specified. Also displayed continuously when KAQM14131-E is displayed.
4	KAQM14138-E	There are too many or too few parameters.	The parameter has excess or deficiency.	After confirming the format of the command, specify the correct parameter, and execute it again.
5	KAQM14150-E	An error occurred in the system.	An error occurred in the system.	Collect the OS log, and send it to the support center. To collect the OS log, refer to “Maintenance Tool ‘2.19 Collecting Logs (oslogget)’ (MNTT 02-1300)”.
6	KAQM14167-W	MegaCLI, which is required to acquire internal hard disk and battery information, is not installed.	Necessary commands to get the information of the built-in disks and batteries are not installed.	Execute again, by installing necessary commands to get the information of the built-in disks and batteries.

Copyright © 2011, 2017, Hitachi, Ltd.

This page is for editorial purpose only.

Copyright © 2014, Hitachi, Ltd.

CONTENTS

B.4 Setting Value when the OS is Installed

Copyright © 2011, Hitachi, Ltd.

This page is for editorial purpose only.

Copyright © 2011, Hitachi, Ltd.

B.4 Setting Value when the OS is Installed

The following shows the setting value that is required when installing OS.
After confirming the following table, return to the status before coming to this operation.

Table B.4-1 Setting Value when the OS is Installed

Item	Setting value
Configuration	If two internal HDDs are installed in the node, ask the system administrator whether it is cluster configuration or single node configuration. If six internal HDDs are installed in the node, it is single node configuration.
User data location	This is not displayed in the cluster configuration. In the single node configuration, Select [1.Internal disk] when not connected to the disk array subsystem, and select [2. External disk] when connected to the disk array subsystem.
Select whether to divide RAID groups for the system LU and for the user LU	This is not displayed in the cluster configuration. This is displayed when [1.Internal disk] is selected as the user data location in the single node configuration. Enter “n” (not to divide.)
RAID rebuilding necessity	This is not displayed in the cluster configuration. In the single node configuration, follow the instruction in the manual because whether RAID rebuilding is necessary or not depends on the recovery procedure.

Copyright © 2011, 2012, Hitachi, Ltd.

This page is for editorial purpose only.

Copyright © 2011, Hitachi, Ltd.

CONTENTS

B.5 Disk Setting

B.5.1 Acquiring WWNs of Nodes

Copyright © 2012, Hitachi, Ltd.

This page is for editorial purpose only.

Copyright © 2012, Hitachi, Ltd.

B.5 Disk Setting

B.5.1 Acquiring WWNs of Nodes

Acquire a WWN of node that is set to HBA BIOS from the KVM console.

This process must be done in each node with switching the console.

For the KVM connection, refer to "Set Up '1.2 Confirmation of KVM Connection' (SETUP 01-0010)".

(1) Execute (a) when OS is stopped, and execute (b) when OS is running.

(a) Startup the OS by refer to "Installation '2.1.1 Procedure for turning on the power' (INST 02-0000)".

(b) Reboot the OS by refer to "Installation '2.1.3 Procedure for rebooting the OS' (INST 02-0100)".

(2) If the following message is displayed while starting up the OS, press [E] key with keep pressing of [Alt] key or [Ctrl] key to display the Emulex Utility window.

```
<Message>
  Press < Alt-E> or <Ctrl-E> to enter Emulex BIOS Configuration utility.
  Press< s > to skip Emulex BIOS
```

(3) Input the port number (1-2) to be acquired WWN in the "Enter a Selection:" on Figure B.5.1-1, then press [Enter] key.
If WWN for all of the installed ports is completed its acquiring, press [x] key and proceed to (5).

NOTE: Figure B.5.1-1 shows an example of the input window when the port number "1" is selected.

```
Emulex Light Pulse BIOS Utility, ZB2.02a2
Copyright (c) 1997-2007 Emulex. All rights reserved.

Emulex Adapters in the System:

1. LPe11002-M4:    PCI Bus, Device, Function (02, 00, 00)
2. LPe11002-M4:    PCI Bus, Device, Function (02, 00, 01)



Enter a Selection: 1

Enter <x> to Exit
```

Figure B.5.1-1 Emulex Utility window when one HBA with 2 Ports are installed (Example)

Copyright © 2012, Hitachi, Ltd.

(4) Take a note of WWN (16-digit alphanumeric characters) displayed at “Port Name:” in Figure B.5.1-2 in the worksheet for a memo of WWN as shown in Table B.5.1-1, and then press [Esc] key to return to the previous window.

```
Adapter 01:          PCI Bus, Device, Function (02, 00, 00)

LPe11002-M4:   I/O Base:2000     Firmware Version: ZS2.72A2
Port Name: 10000000 C988752A     Node Name: 20000000 C988752A
Topology: Auto Topology : Loop First (Default)
The BIOS of this Adapter is Disable

1.  Configure Boot Devices
2.  Configure This Adapter’s Parameters



Enter a Selection:

Enter <x> to Exit        <d> to Default Values        <Esc> to Previous Menu
```

Figure B.5.1-2 Emulex Utility port window (Example)when 1 HBA with 2 Ports are Mounted

NOTE: The column in Table B.5.1-1 is listed from the left in the order of “1.” and “2.” in Figure B.5.1-1.

Table B.5.1-1 Example of Writing Worksheet for Memo of WWN when the port number of node 0 is “1”.

	PCI Bus, Device, Function (02, 00, 00)	PCI Bus, Device, Function (02, 00, 01)
node0	10000000 C988752A	
node1		

(5) Execute (3) to (4) to the number of installed ports.

(6) Enter “Y” to the message of “REBOOT THE SYSTEM (Y/N);” in Figure B.5.1-3.

```
Reboot the System to make All the Changes to Take Effect!

REBOOT THE SYSTEM (Y/N);
```

Figure B.5.1-3 Reboot message

(7) Node is rebooted automatically when entering “Y”.

Copyright © 2012, Hitachi, Ltd.

CONTENTS

C.1 Local Initial Operations According to Maintenance Request

C.1.1 When Detected by HiTrack

C.1.2 When Detected by SNMP Trap

C.1.3 When the System Administrator Noticed a Failure

C.1.3.1 Action to be taken in the cluster configuration

C.1.3.2 Action to be taken it the single node configuration

C.1.4 When the Maintenance Personnel Noticed the Failure at the Time of Initial Installation in the Local Site

C.1.5 Determination Procedure for the Possible Failure Part when a PCI Error Occurred

Copyright © 2011, 2013, Hitachi, Ltd.

This page is for editorial purpose only.

Copyright © 2011, 2013, Hitachi, Ltd.

C.1 Local Initial Operations According to Maintenance Request

Before troubleshooting, this chapter describes precautions for maintenance personnel to refer to maintenance procedures in HA8000 maintenance manual partly.

Determination of a failure and parts replacement of Hitachi Data Ingestor (HDI) hardware are performed with reference to both the HDI maintenance manual and the HA8000 maintenance manual for which maintenance personnel need to do a certain amount of work in the HA8000 maintenance manual first and return to the work in the HDI maintenance manual.

Figure C.1-1 shows general flow for the maintenance personnel to refer to the proper procedures described in the two maintenance manuals while performing troubleshooting or parts replacement of HDI hardware.

The maintenance personnel must refer to and understand the flow in Figure C.1-1 before performing troubleshooting or parts replacement.

Copyright © 2011, 2013, Hitachi, Ltd.

Troubleshooting or parts replacement policy using two manuals (*)

- ✓ Start a failure determination with HDI maintenance manual.
- ✓ Determine a failure by HATP if node is down; determine a failure by SIM of the OS if node is running.
- ✓ Do not refer to the parts replacement procedure of HA8000 maintenance manual from the result of the failure determination of HA8000 maintenance manual; return to the caller of HDI maintenance manual and follow the instruction.
- ✓ If the node did not recover from the failure after part replacement, determine the failure again.

*: "Two manuals" indicates HDI maintenance manual and HA8000 maintenance manual.

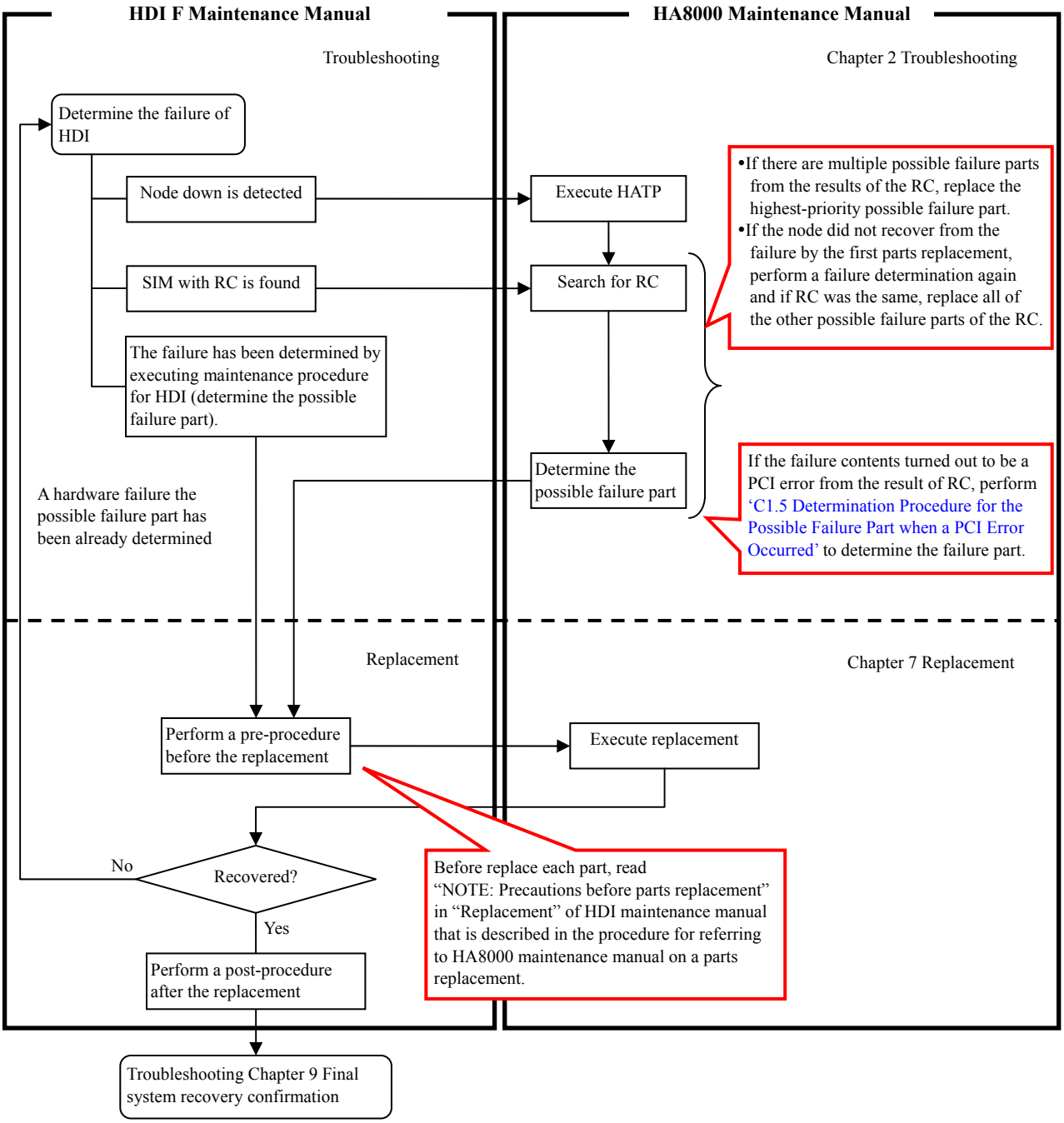


Figure C.1.1 General Flow for Referring to Procedures in Two Manuals

Copyright © 2012, 2013, Hitachi, Ltd.

C.1.1 When Detected by HiTrack

A failure detected by HiTrack is reported to the Maintenance Center of (HDS) by HiTrack. The maintenance personnel should perform the failure analysis according to the following.

(1) Receive the failure information acquired by HiTrack from the Maintenance Center of (HDS) via FTP or e-mail.

(2) Acquire TagID and SIM from the received failure information.
The acquired TagID is used in the failure analysis to specify the failure occurrence node and to replace the parts. The acquired SIM is used in the failure analysis to analyze the failure of Hitachi Data Ingestor.

NOTE: The acquired SIM is the one when the failure occurred or when the communication with the node was disrupted.
Maintenance personnel need to confirm the SIM by connecting the maintenance PC even at the local site.

(3) Based on the acquired TagID and SIM, perform the failure analysis and failure determination operation.
For the details of the failure analysis and the failure determination operation, refer to 'C.2.2 Determination Procedure when a Failure Occurred'.

Copyright © 2012, 2013, Hitachi, Ltd.

C.1.2 When Detected by SNMP Trap

When monitoring by SNMP, a failure detected by HDI is stored in the SNMP Trap server as a failure information equivalent to SIM and reported to the SNMP manager. After that, it is reported to the Maintenance Center of (HDS) by the system administrator. The maintenance personnel should perform the local initial measurement and failure analysis according to the following.

(1) By requesting the system administrator, receive all the SNMP Trap. Maintenance personnel should check the Trap IDs and Trap messages in the received SNMP Trap, and check whether there is a Trap where the SIM of HDI is stored or not. For the details of SNMP Trap where the SIM of HDI is stored, refer to "Troubleshooting '7.2 Messages of Trap that the Maintenance Personnel should Obtain Table 7.2-1 SNMP Trap to be sent by HDI' (TRBL 07-0010).

(2) Based on the management IP address (IP address of the port used in the operation in the single node configuration) of the received failure information, confirm the position of the node where a failure occurred with the system administrator. The confirmed position of the node where a failure occurred is used in the failure analysis for specifying the failure occurrence location and for replacing.
In the single node configuration, the system administrator should execute the failure determination that is described in 'C.1.3 When the System Administrator Noticed a Failure' in advance.
However, if the "KAQK37525-E" SIM message ID is included in the "KAQG46040-E" that is received Trap ID of SNMP Trap, there is a possibility that the system data or the user data has been lost. In this case, it is needed to execute the initial installation of OS and to restore the data from the backup information. For this reason, execute the Table C.1.2-1 or Table C.1.2-2 according to the configuration.

(3) Based on the collected failure information, perform the failure analysis and failure determination operation. For the details of the failure analysis and failure determination operation, refer to 'C.2.2 Determination Procedure when a Failure Occurred'.

Table C.1.2-1 Procedures for restoring data in the node in the configuration using management port

#	Contents	Worker
1	Execute the initial OS installation (with RAID reconfiguration) (*1)	Maintenance personnel
2	Execute setup after installation is completed.	Maintenance personnel
3	Execute the restoration of the system LU (including user data)	System administrator
4	Confirm that no error message related to the file system or the file sharing is output	System administrator
5	In the HDI for Cloud configuration, confirm if the file configuration is consistent between the HDI and the HCP after performing the restoration by using the CLI command which is open to the system administrator.	System administrator
6	Execute the I/O confirmation for the system	System administrator

*1: All data within the node will be initialized.

Copyright © 2011, 2013, Hitachi, Ltd.

Table C.1.2-2 Procedures for restoring data in the node in the configuration using trunk 2 Data ports

#	Contents	Worker
1	Ask the system administrator to search a vacant port of IP-SW of front-end LAN, then connect the Management port of the node to the vacant port with a LAN cable.	Maintenance personnel
2	Execute the initial OS installation (with RAID reconfiguration) (*1)	Maintenance personnel
3	Execute setup after installation is complete (Set the IP address and Routing used for trunk 2 data ports in the front-end LAN to the Management port IP address. (Ask the system administrator about the IP address and Routing for trunk 2 data ports in the front-end LAN.)	Maintenance personnel
4	Execute the restoration of the system LU (including user data)	System administrator
5	After the restoration is completed, remove the LAN cable between IP-SW of front-end LAN and the Management port that was connected at sequence #1 of the node .	Maintenance personnel
6	Confirm that no error message related to the file system or the file sharing is output	System administrator
7	In the HDI for Cloud configuration, confirm if the file configuration is consistent between the HDI and the HCP after performing the restoration by using the CLI command which is open to the system administrator.	System administrator
8	Execute the I/O confirmation for the system	System administrator

*1: All data within the node will be initialized.

Copyright © 2011, 2013, Hitachi, Ltd.

C.1.3 When the System Administrator Noticed a Failure

When the system administrator detected a failure, it is reported to the Maintenance Center of (HDS) by the system administrator. The maintenance personnel should perform the local initial measurement and failure analysis according to the following.
In the single node configuration, the system administrator should determine a failure in advance to make shorten of downtime.
Refer to C.1.3.1 Action to be taken in the cluster configuration for the cluster configuration and 'C.1.3.2 Action to be taken it the single node configuration' for the single node configuration.

C.1.3.1 Action to be taken in the cluster configuration

(1) When the failure noticed by the system administrator is the ERROR lamp lighting of the node or LED alarm lighting of the parts (power unit, embedded HDD and others)

① Request the system administrator to check the status of the LCD display and LED alarm lighting of the installed parts.

② The confirmed information is used in the failure analysis.

③ Based on the collected failure information, perform the failure analysis and failure determination operation. For the details of the failure analysis and failure determination operation, refer to 'C.2.2 Determination Procedure when a Failure Occurred'.

(2) When the failure noticed by the system administrator is the abnormal OS operation and inaccessible
Request the system administrator if he/she can access the both node with HFSM, and if it can be accessed, check whether failover has occurred or not.

- Proceed to (2-1) if the system administrator cannot access the both nodes with HFSM and installing the management LAN IP-SW provided by (HDS).
- If the management LAN IP-SW owned by the customer is installed, request the customer to determine the failure.
- When the failover has occurred, proceed to step (2-2).
- When the failover has not occurred, proceed to step (2-3).

(2-1) When it cannot access the both nodes with HFSM

① Remove the LAN cable connected to the #7 port on the management LAN IP-SW, and connect the removed LAN cable to the #9 port on the management LAN IP-SW. Request the system administrator to check whether it can communicate with the both nodes with HFSM.
When it is available to communicate, execute the step② to step⑤. When it is not available to communicate, reconnect the removed LAN cable to the port as it was connected, and execute the step⑥.

② Because it is the port failure of the maintenance LAN IP-SW, ask the system administrator to failover the resource group. If the system administrator is not available to operate, maintenance personnel should perform this operation with the permission of the system administrator. Ask the system administrator which node should be used to failover the resource group. If no instruction is given, failover the resource group on the node 1 to the node 0. For the failover procedure, refer to "Maintenance Tool '3.1 Failover Node Termination to Execute the OS stop or OS reboot' (MNTT 03-0000)".

③ Remove the #3 port on the maintenance LAN IP-SW that is connected with the management port on the side of node1, and remove the LAN cable that is connected with the management port on the side of node0.

④ Connect the LAN cable that is removed from #3 on the maintenance LAN IP-SW at the step③ to the management port on the side of node0.

Copyright © 2011, 2015, Hitachi, Ltd.

⑤ Replace the management LAN IP-SW. For the replacement of management LAN IP-SW, refer to "Replacement '1.6 Replacing the Management LAN IP-SW (IP Switch)' (REP 01-0280)".
After replacing the management LAN IP-SW, execute the operation described in "Troubleshooting '9.1.2 Confirmation of Recovery from Hardware Failure' (TRBL 09-0010)".

⑥ Request the system administrator to replace the LAN cable that is connected between the HFSM and the management LAN IP-SW, and check if the connection can communicate or not.
If it cannot communicate, it is a failure of the management server. Therefore, request the system administrator to review and replace the management server.

(2-2) When failover has occurred

① Request the system administrator to check SIM. The confirmed SIM is used in the failure analysis.

② Based on the collected failure information, perform the failure analysis and failure determination operation. For the details of the failure analysis and failure determination operation, refer to 'C.2.2 Determination Procedure when a Failure Occurred'.

(2-3) When failover has not occurred

① The system administrator may have performed the incorrect setting. Request the system administrator to recheck the items before and after the setting if there are any errors or not.

② Request the system administrator to acquire the failure information.

③ Execute the manual dump operation. Furthermore, inform the Technical Support Center of the manual dump execution.

④ Send the acquired failure information to the Technical Support Center via e-mail.

Copyright © 2011, 2015, Hitachi, Ltd.

C.1.3.2 Action to be taken it the single node configuration

(1) In the single node configuration, maintenance personnel get the result of failure determination operation from the system administrator, and execute the action to be taken according to the result. Figure C.1.3.2-1 shows the overview of the determination flow to be executed by the system administrator.

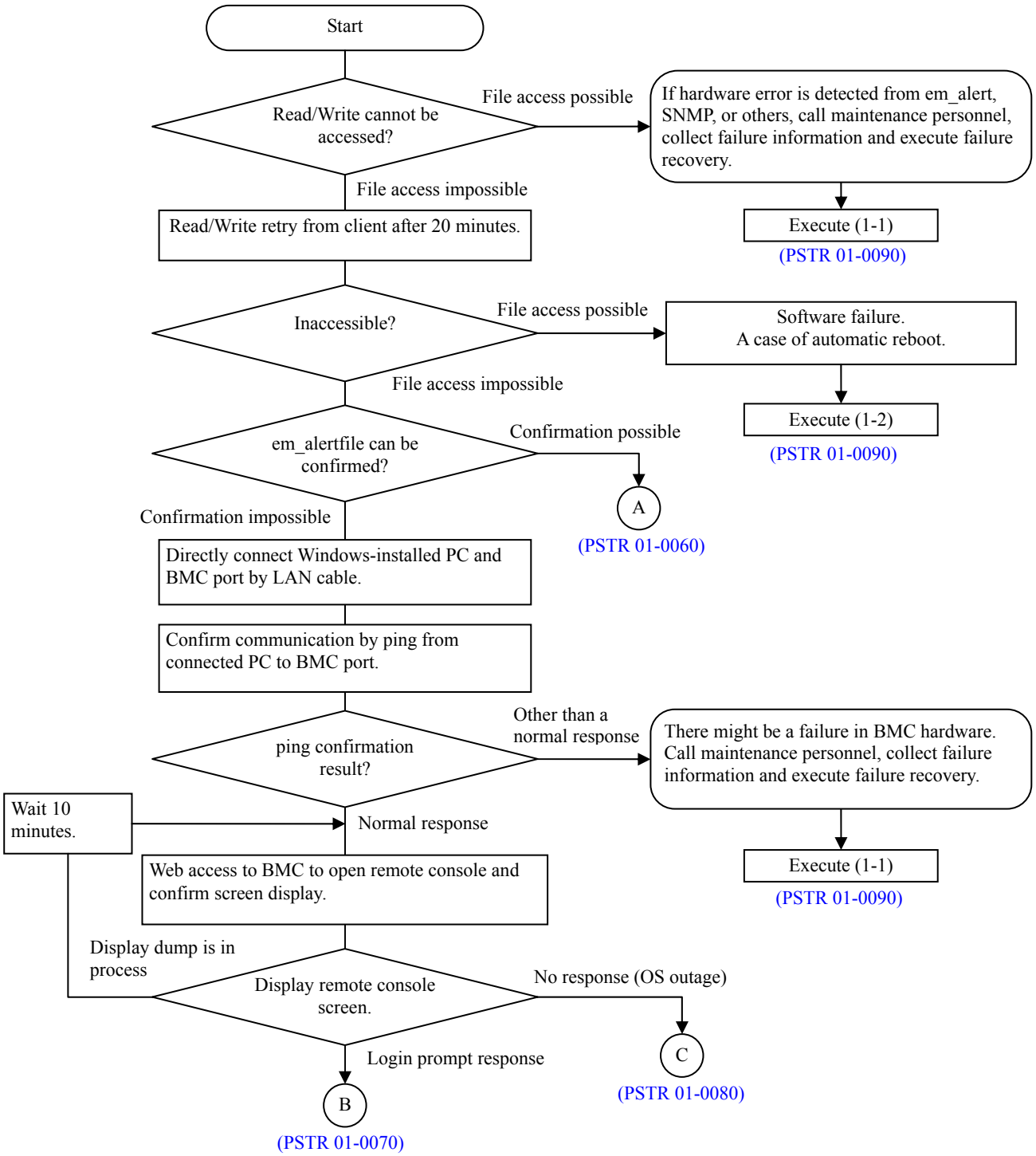


Figure C.1.3.2-1 Overview of Determination Flow by System Administrator (1/4)

Copyright © 2011, 2013, Hitachi, Ltd.

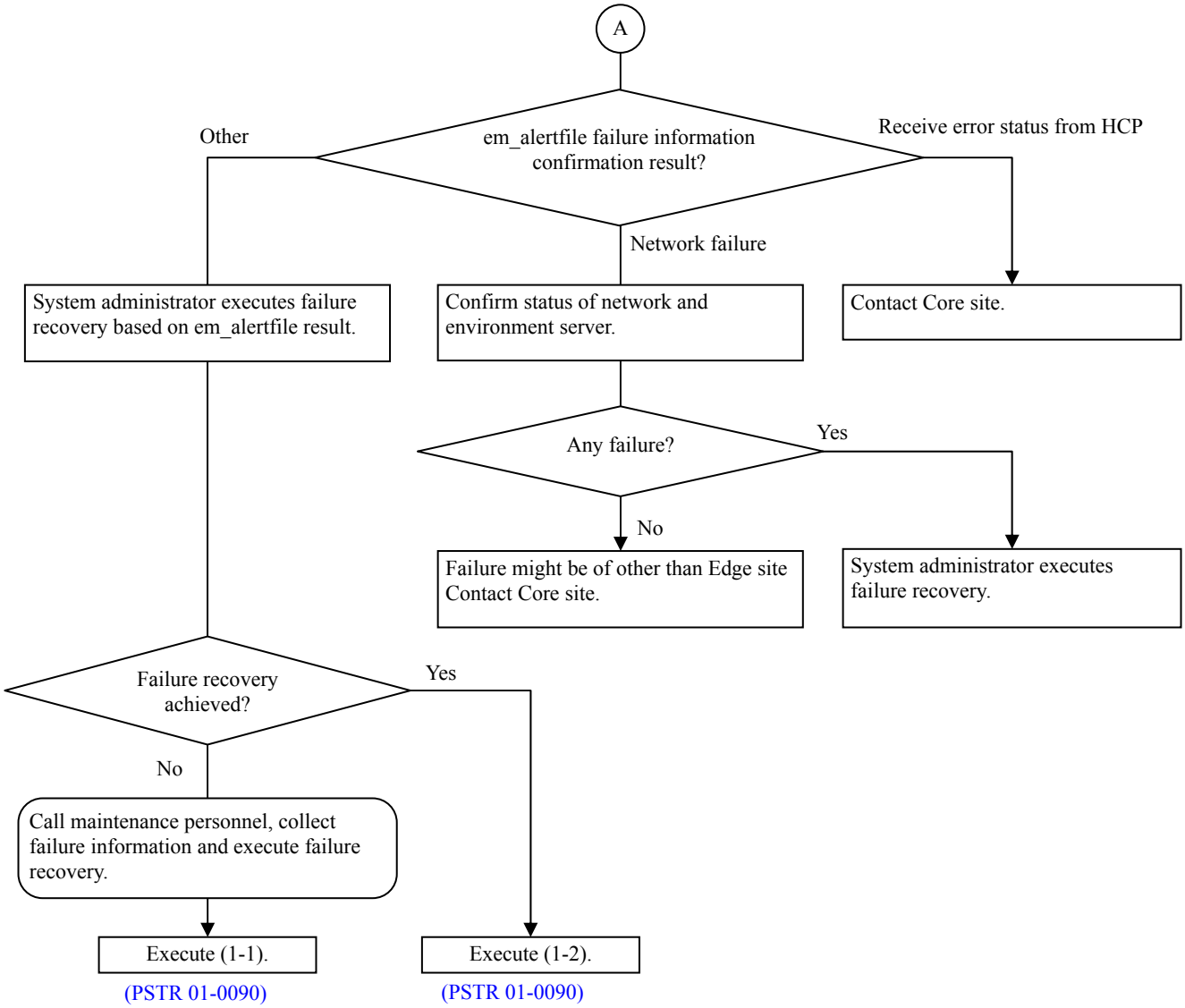


Figure C.1.3.2-1 Overview of Determination Flow by System Administrator (2/4)

Copyright © 2011, 2013, Hitachi, Ltd.

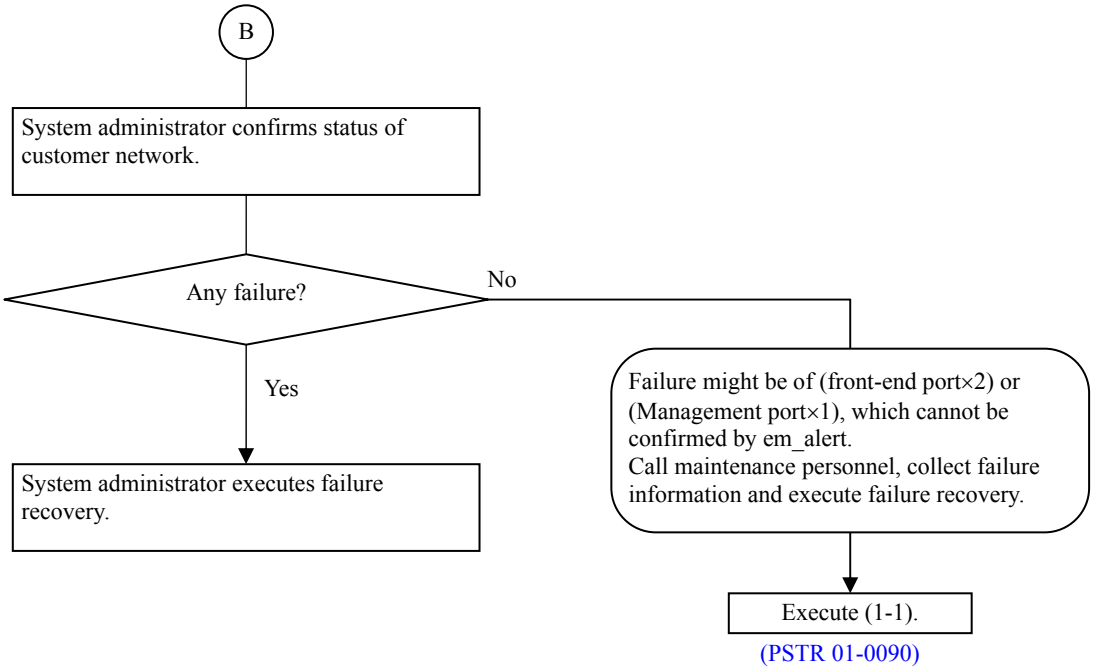


Figure C.1.3.2-1 Overview of Determination Flow by System Administrator (3/4)

Copyright © 2011, 2013, Hitachi, Ltd.

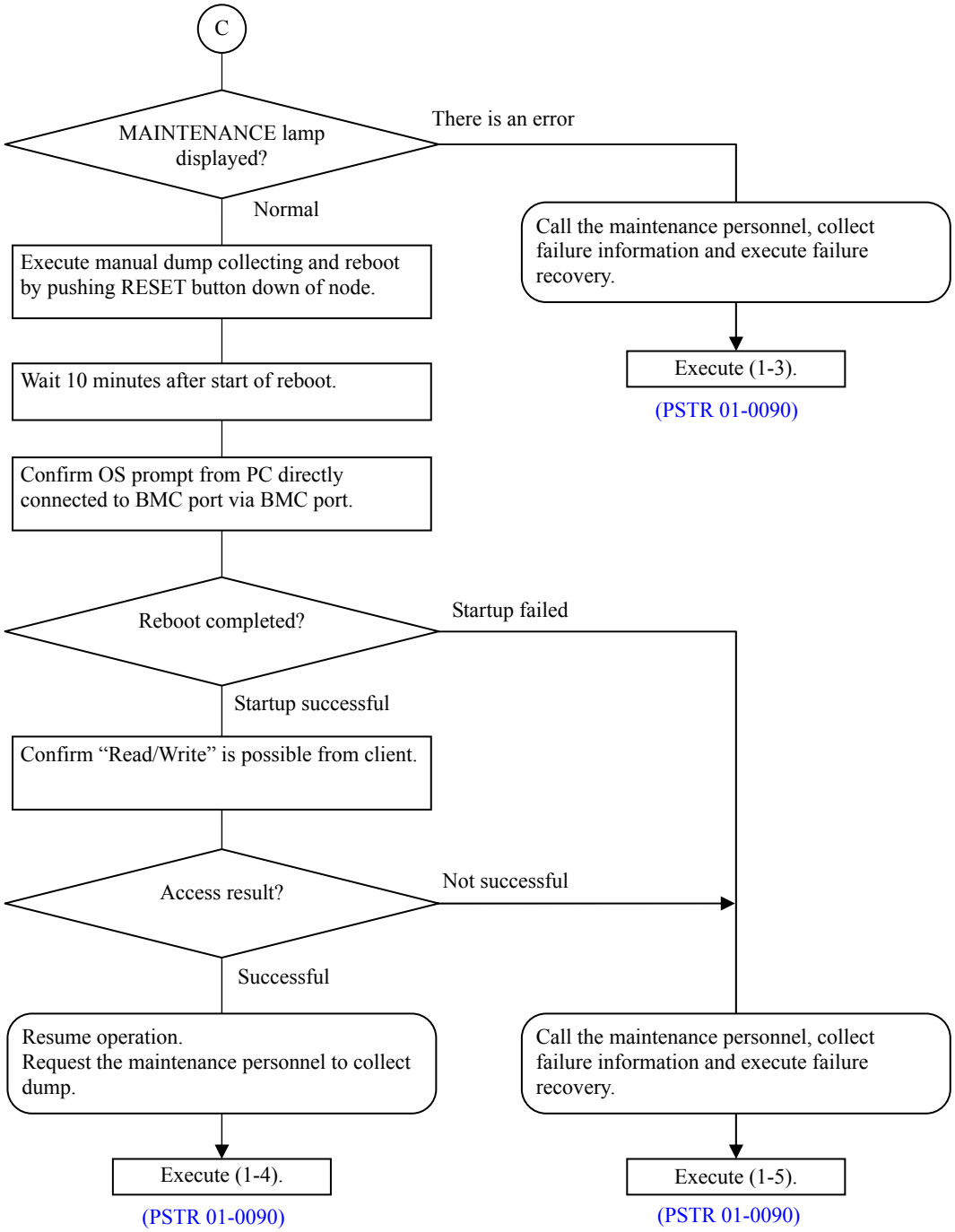


Figure C.1.3.2-1 Overview of Determination Flow by System Administrator (4/4)

Copyright © 2011, 2013, Hitachi, Ltd.

(1-1) OS is running, and when the system administrator cannot restore from the failure information (such as em_alert/SNMP Trap).
Execute failure analysis and the failure determination based on the collected failure information.
Refer to 'C.2.2 Determination Procedure when a Failure Occurred' for the details of failure analysis and determination process of a failure.

(1-2) OS is running, and when the system administrator can be restored from the failure information (such as em_alert/SNMP Trap).
Because the restarting operation is available, collect the failure information from the system administrator.

(1-3) It cannot confirm that the OS is running or not, and the MAINTENANCE lamp display of a node shows an error.
Execute failure analysis and the failure determination based on the collected failure information.
Refer to 'C.2.2 Determination Procedure when a Failure Occurred' for the details of failure analysis and determination process of a failure.

(1-4) When the system administrator executes the dump manually and then after collecting the dump manually, the system starts automatically and confirmed that the I/O operation is available (This is executed when it is unknown if the OS is running and the MAINTENANCE lamp display shows normal.)
Because the restarting operation is available, collect the failure information from the system administrator.

(1-5) After collecting the dump manually by the system administrator, the system does not start automatically or the I/O operation cannot be done after restarting. (This is executed when it is unknown if the OS is running and the MAINTENANCE lamp display shows normal.)
Execute failure determination operation.
Refer to 'C.2.2 Determination Procedure when a Failure Occurred' for the details of failure analysis and determination process of a failure.

Copyright © 2011, 2013, Hitachi, Ltd.

C.1.4 When the Maintenance Personnel Noticed the Failure at the Time of Initial Installation in the Local Site

When the maintenance personnel noticed the ERROR lamp lighting and the LED lighting of the parts of the node in which the failure occurred, perform the local initial measurement and failure analysis according to the following.

(1) Check the alarm lighting of the installed parts and others of the node in which the failure occurred.

(2) Perform “hwstatus” for the node in which the failure occurred.
For the details of “hwstatus”, refer to ‘B.3.1 Displaying the Hardware Status (hwstatus)’.

(3) Acquire the result of “hwstatus”. Note that the connection (remote node BMC connection status) of BMC Information becomes “none” (cluster not built) at the time of initial installation because it is before the cluster building.

(4) Based on the result of “hwstatus”, replace the failure occurrence parts of the failure occurrence node.
For the details of the part replacement, refer to “Replacement ‘Chapter 1 Replacing the Components of Hitachi Data Ingestor’ (REP 01-0000)”.

Copyright © 2011, 2013, Hitachi, Ltd.

C.1.5 Determination Procedure for the Possible Failure Part when a PCI Error Occurred

If SIM message in a failure notice is “KAQK30801-E”, the failure content can be determined by RC information which is included in the SIM message.

Although, in the case the failure content of RC turns out to be a PCI error, RC information alone is not enough to determine the possible failure part; the combination of installation pattern of PCI slot and SEL information is required in that case.

RC of a PCI error is either of the following.

1001000A13E46FA4XXXXXXXX (Parity error of PCI)

1001000A13E56FA5XXXXXXXX (System error of PCI)

The determination procedure of a possible failure part when a PCI error occurred is as follows.

Note that the following software must be installed on the maintenance PC by the maintenance personnel in advance.

Extraction software (software that can extract “tar.gz”)

Text editor (Notepad is acceptable)

The following shows the determination procedure of a possible failure part.

In the case the maintenance personnel collect logs, perform (1) to (3) of [In the case the maintenance personnel collect logs], and in the case you receives logs collected from HFSM by the system administrator, perform (1) to (3) of [In the case the system administrator collected logs], then perform procedure (4) and subsequent procedures in both cases.

[In the case the maintenance personnel collect logs]

(1) Execute oslogget command on the node where a SIM with RC of PCI error was output to download logs onto the maintenance PC. This procedure is not necessary if logs have been already downloaded.
For oslogget command, refer to “Maintenance Tool ‘2.19 Collecting Logs (oslogget)’ (MNTT 02-1300)”.

(2) Extract the log which was downloaded in the procedure (1) on the maintenance PC with the extraction software.

(3) Open the extracted log folder “naslog_full_nncX” (X: the node on which the command was executed) and extract “selmanager.tar.gz.”

[In the case the system administrator collected logs]

(1) Confirm that ALL log you received from the system administrator is the log of the node from which a SIM with RC of PCI error was output.

(2) Extract ALL log received in procedure (1) on the maintenance PC with the extraction software.

(3) Open the extracted log folder and search by “selmanager.tar.gz” inside the folder, and then extract the hit file. (“selmanager.tar.gz” is stored under “var\log.”)

Copyright © 2012, 2013, Hitachi, Ltd.

(4) Open the extracted “opt” folder and open “ipmi_sel.log” stored under “opt\hitachi\SelManager” with the text editor.

(5) Search in the opened file by the specified characters below and check the hit SEL.
Use these two specified characters for the search. (*)
01000413E46FA4
01000413E56FA5

*: The search must be performed for the both specified characters because the SEL format of a PCI error is either of the following.
“xxxx02yyyymmdd01000413E46FA4zzzz”
“xxxx02yyyymmdd01000413E56FA5zzzz”
xxxx: Record ID yyyymmdd: Time stamp zzzz: bus/device/function

(6) Note down the last 4 digits of SEL that was hit in procedure (5).
“zzzz” in SEL formats above is the part to be noted.
In the case two or more SEL were hit in procedure (5), note down the last 4 digits of all the hit SEL.

(7) Check the back side of the node to confirm which pattern in Table C.1.5-1 corresponds to the current PCI installation status.

Table C.1.5-1 PCI Slot Installation List

#	Slot 1	Slot 2	Slot 4	Installation pattern
1	GbE-2Portcard	Fibre Channel card	—	Pattern 0
2	GbE-2Port card	—	—	
3	GbE-2Port card	Fibre Channel card	GbE-4Port card	Pattern 1

*: Slot 3 and Slot 5 is always empty (no card is installed).

(8) Use a list for possible failure part of determination either Table C.1.5-2 or Table C.1.5-3 of which the installation pattern corresponds to the one you confirmed in procedure (7). Find the line in the list where “Last 4 bytes in SEL” is same as the last 4 digits of SEL that was noted down in procedure (6).
The first possible failure part in the line you have determined is the first replacement part.
If the node did not recovered from the error after the replacement of the first possible failure part, replace all the parts described in the second and the third possible failure part.

Copyright © 2012, 2013, Hitachi, Ltd.

Table C.1.5-2 List for Possible Failure Part Determination in the case of Installation Pattern 0

#	Last 4 bytes in SEL	First possible failure part	Second possible failure part	Third possible failure part
1	0000	Motherboard	—	—
2	0008	Motherboard	PCI Riser B Board	Card installed in slot 1
3	0038	Motherboard	PCI Riser B Board	Card installed in slot 2
4	0048	Motherboard	RAID controller	—
5	00A0	Motherboard	—	—
6	00A1	Motherboard	—	—
7	00A2	Motherboard	—	—
8	00B0	Motherboard	—	—
9	00B1	Motherboard	—	—
10	00B2	Motherboard	—	—
11	00B3	Motherboard	—	—
12	00B4	Motherboard	—	—
13	00B5	Motherboard	—	—
14	00B6	Motherboard	—	—
15	00B7	Motherboard	—	—
16	00D0	Motherboard	—	—
17	00D1	Motherboard	—	—
18	00D7	Motherboard	—	—
19	00E0	Motherboard	—	—
20	00E4	Motherboard	—	—
21	00E5	Motherboard	—	—
22	00E8	Motherboard	USB device (*1)	—
23	00E9	Motherboard	USB device (*1)	—
24	00EA	Motherboard	USB device (*1)	—
25	00EB	Motherboard	USB device (*1)	—
26	00EF	Motherboard	USB device (*1)	—
27	00F0	Motherboard	—	—
28	00F8	Motherboard	—	—
29	00FA	Motherboard	—	—
30	00FB	Motherboard	—	—
31	0100	Card installed in slot 1	PCI Riser B Board	Motherboard
32	0101	Card installed in slot 1	PCI Riser B Board	Motherboard
33	0400	Card installed in slot 2	PCI Riser B Board	Motherboard
34	0401	Card installed in slot 2	PCI Riser B Board	Motherboard
35	0500	RAID controller	Motherboard	—
36	0600	Motherboard	—	—
37	0601	Motherboard	—	—
38	0700	Motherboard	—	—

*1: “USB device” means a device connected with USB.

Copyright © 2012, 2013, Hitachi, Ltd.

Table C.1.5-3 List for Possible Failure Part Determination in the case of Installation Pattern 1

#	Last 4 bytes in SEL	First possible failure part	Second possible failure part	Third possible failure part
1	0000	Motherboard	—	—
2	0008	Motherboard	PCI Riser B Board	Card installed in slot 1
3	0028	Motherboard	PCI Riser A Board	Card installed in slot 4
4	0038	Motherboard	PCI Riser B Board	Card installed in slot 2
5	0048	Motherboard	RAID controller	—
6	00A0	Motherboard	—	—
7	00A1	Motherboard	—	—
8	00A2	Motherboard	—	—
9	00B0	Motherboard	—	—
10	00B1	Motherboard	—	—
11	00B2	Motherboard	—	—
12	00B3	Motherboard	—	—
13	00B4	Motherboard	—	—
14	00B5	Motherboard	—	—
15	00B6	Motherboard	—	—
16	00B7	Motherboard	—	—
17	00D0	Motherboard	—	—
18	00D1	Motherboard	—	—
19	00D7	Motherboard	—	—
20	00E0	Motherboard	—	—
21	00E4	Motherboard	—	—
22	00E5	Motherboard	—	—
23	00E8	Motherboard	USB device (*1)	—
24	00E9	Motherboard	USB device (*1)	—
25	00EA	Motherboard	USB device (*1)	—
26	00EB	Motherboard	USB device (*1)	—
27	00EF	Motherboard	USB device (*1)	—
28	00F0	Motherboard	—	—
29	00F8	Motherboard	—	—
30	00FA	Motherboard	—	—
31	00FB	Motherboard	—	—
32	0100	Card installed in slot 1	PCI Riser B Board	Motherboard
33	0101	Card installed in slot 1	PCI Riser B Board	Motherboard
34	0600	Card installed in slot 4	PCI Riser A Board	Motherboard
35	0710	Card installed in slot 4	PCI Riser A Board	Motherboard
36	0720	Card installed in slot 4	PCI Riser A Board	Motherboard
37	0800	Card installed in slot 4	PCI Riser A Board	Motherboard
38	0801	Card installed in slot 4	PCI Riser A Board	Motherboard
39	0900	Card installed in slot 4	PCI Riser A Board	Motherboard
40	0901	Card installed in slot 4	PCI Riser A Board	Motherboard
41	0A00	Card installed in slot 2	PCI Riser B Board	Motherboard
42	0A01	Card installed in slot 2	PCI Riser B Board	Motherboard
43	0B00	RAID controller	Motherboard	—
44	0C00	Motherboard	—	—
45	0C01	Motherboard	—	—
46	0D00	Motherboard	—	—

*1: “USB device” means a device connected with USB.

Copyright © 2012, 2013, Hitachi, Ltd.

This page is for editorial purpose only.

Copyright © 2011, 2013, Hitachi, Ltd.

CONTENTS

C.2 Failure Determination Procedure

C.2.1 Procedures of Troubleshooting at the Time of Setup
C.2.2 Determination Procedure when a Failure Occurred
C.2.2.1 Failure determination procedure at the cluster configuration
C.2.2.2 Failure determination procedure at the single node configuration
C.2.3 Detailed Determination Procedure in Each Failure
C.2.3.1 Procedure for determining power supply failures
C.2.3.1.1 Procedure for determining power supply failures in the cluster configuration
C.2.3.1.2 Procedure for determining power supply failures at the single node configuration
C.2.3.2 Determination of management network failure
C.2.3.2.1 Failure determination by ping command execution result
C.2.3.2.2 Flow of management network failure determination
C.2.3.2.3 Failure determination in case of node outage
C.2.3.3 Determining the node failure when no failover occurs
C.2.3.4 Determining the node failure when failover occurred
C.2.3.5 Determination of node failure in the single node configuration
C.2.3.6 Determination of network failure
C.2.4 Diagnosis for OS Boot Failure

Copyright © 2011, 2013, Hitachi, Ltd.

This page is for editorial purpose only.

Copyright © 2011, 2013, Hitachi, Ltd.

C.2 Failure Determination Procedure

C.2.1 Procedures of Troubleshooting at the Time of Setup

(1) Figure C.2.1-1 shows the flowchart when message IDs described in Table C.2.1-1 are output due to the failure of new installation or the failure of update installation.

Table C.2.1-1 List of Message IDs (1)

Message ID	KAQG61007-E KAQG61008-E KAQG61010-E KAQG61025-E KAQG61027-E

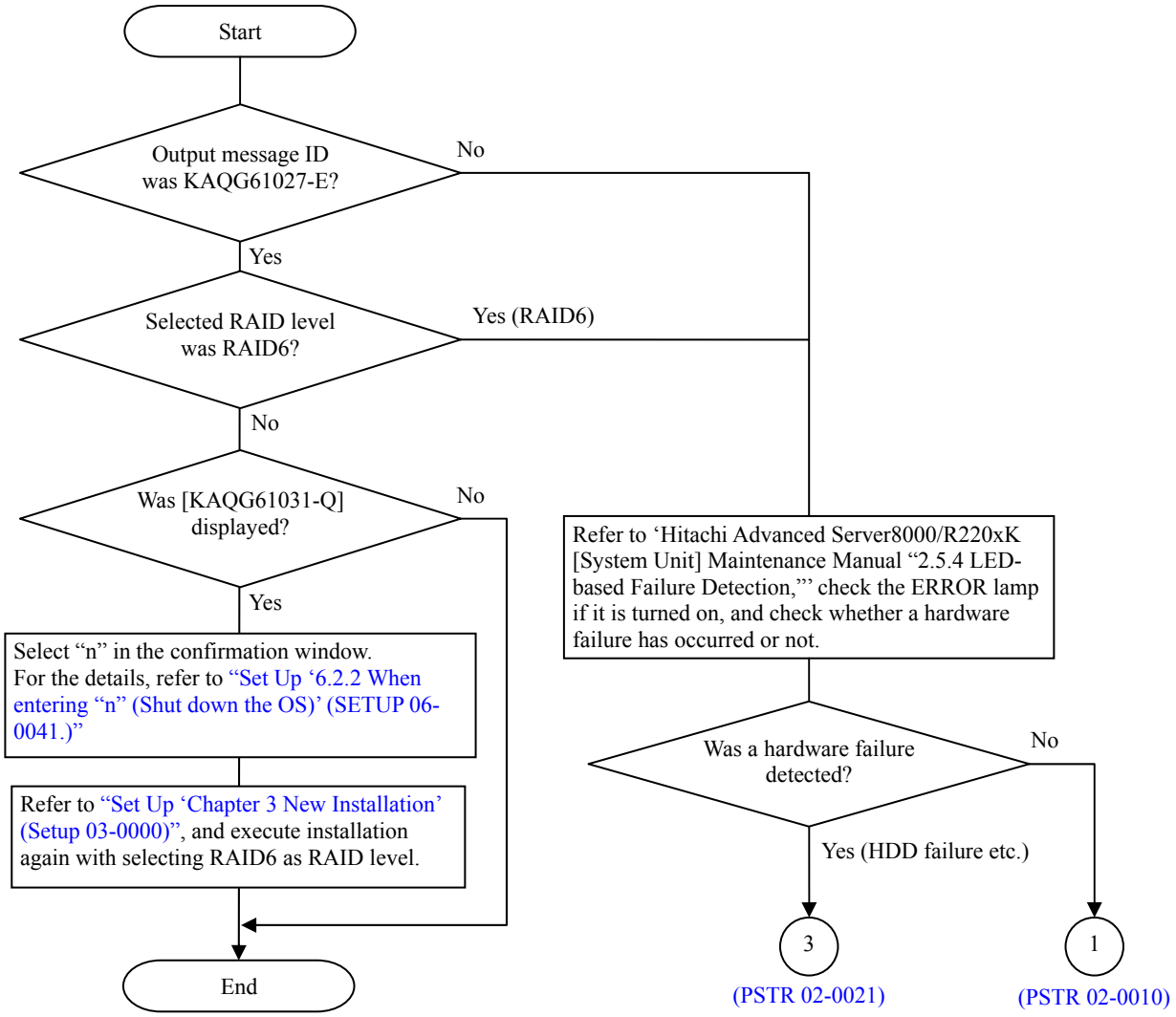


Figure C.2.1-1 Flow of Diagnosis for the Media Failure (1/4)

Copyright © 2011, 2013, Hitachi, Ltd.

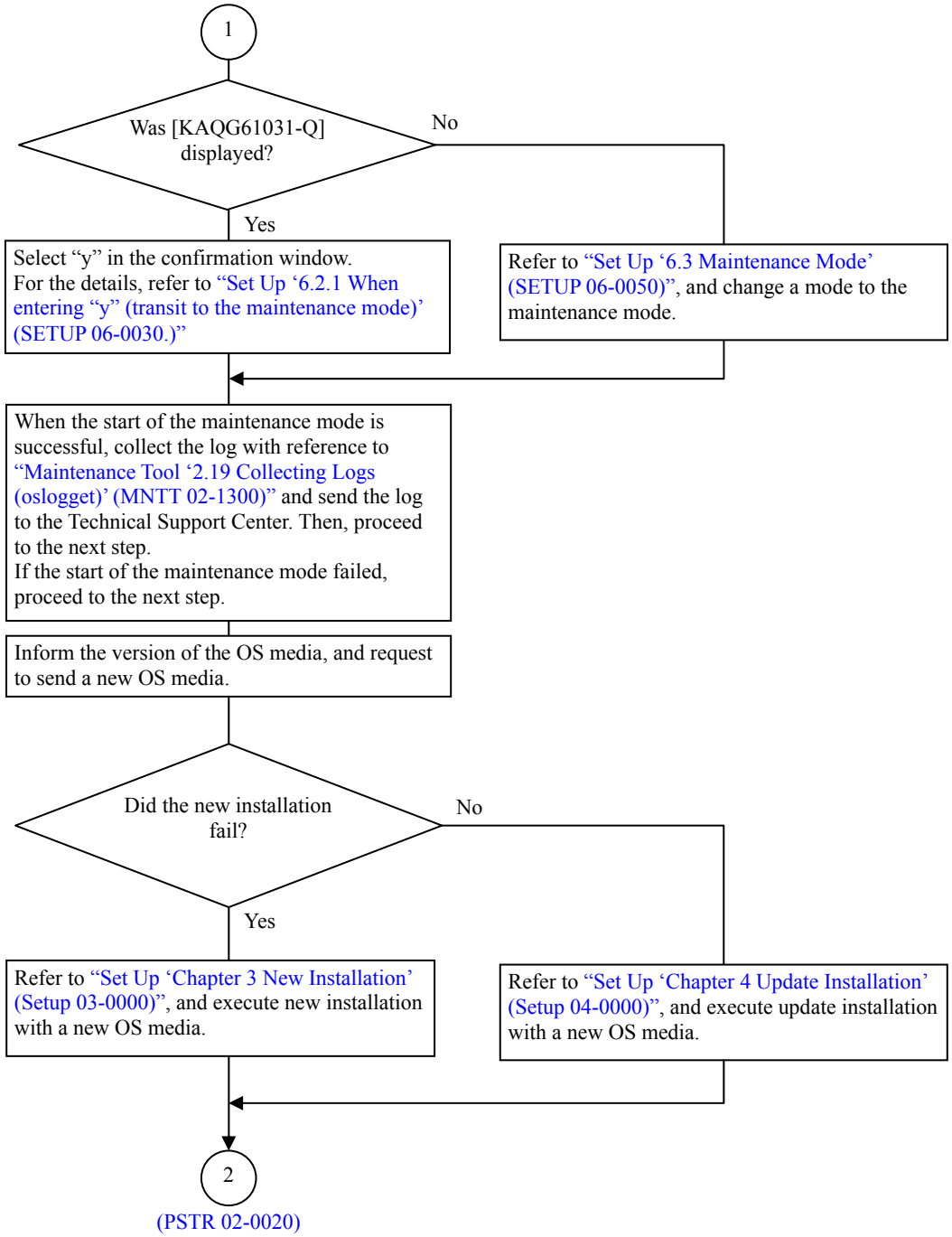


Figure C.2.1-1 Flow of Diagnosis for Media Failure (2/4)

Copyright © 2012, 2014, Hitachi, Ltd.

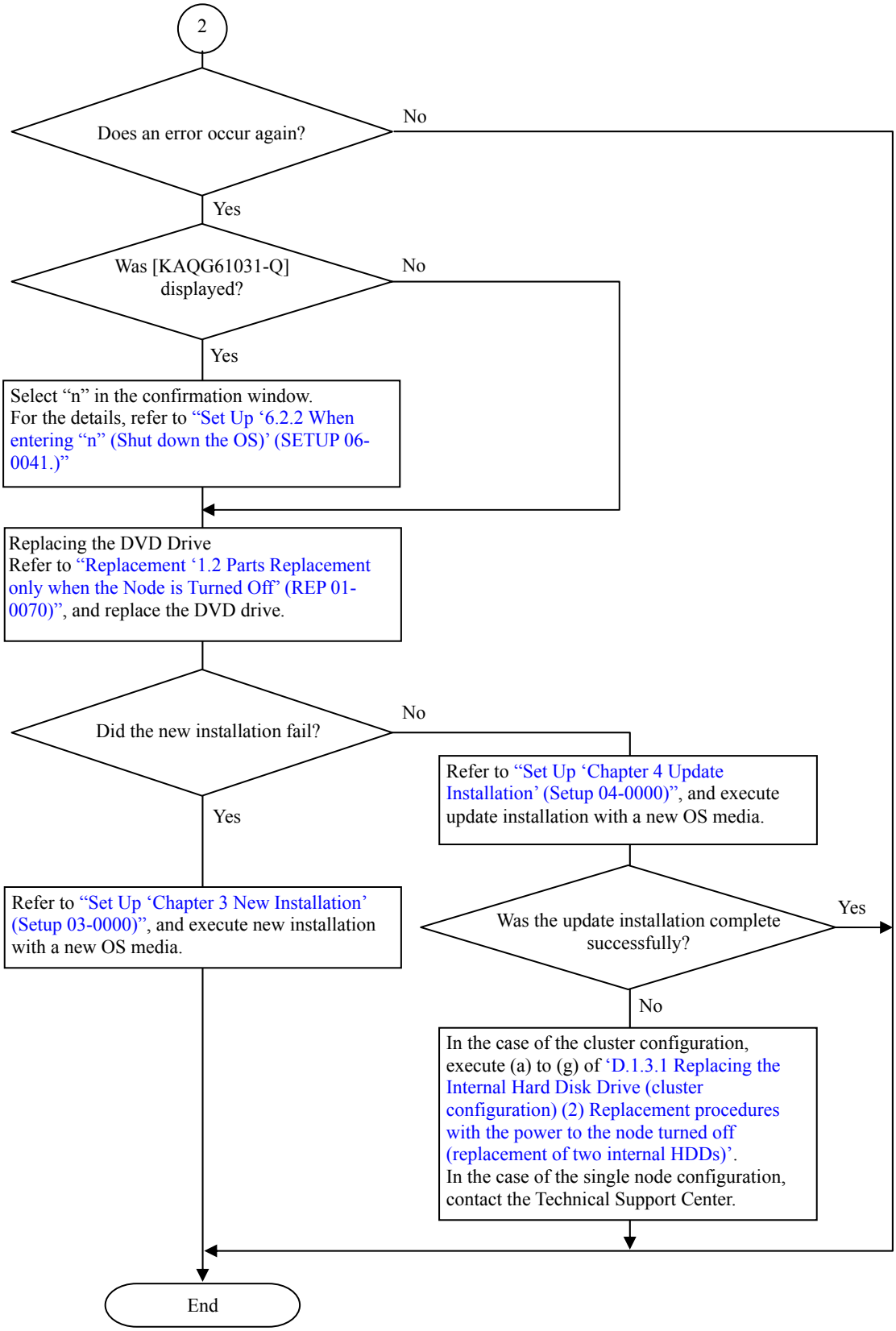
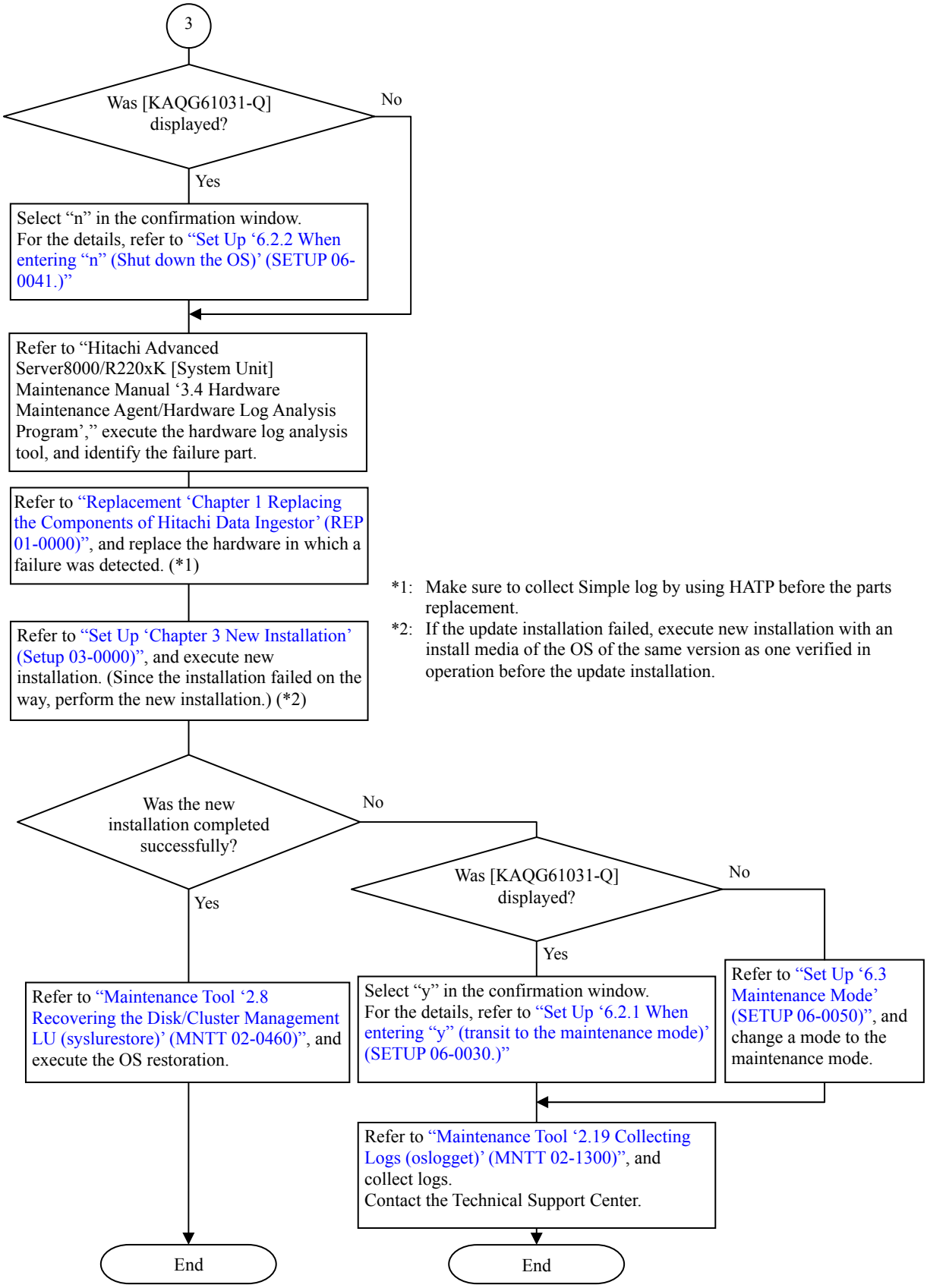


Figure C.2.1-1 Flow of Diagnosis for Media Failure (3/4)

Copyright © 2011, 2013, Hitachi, Ltd.



*1: Make sure to collect Simple log by using HATP before the parts replacement.

*2: If the update installation failed, execute new installation with an install media of the OS of the same version as one verified in operation before the update installation.

Figure C.2.1-1 Flow of Diagnosis for Media Failure (4/4)

Copyright © 2012, 2014, Hitachi, Ltd.

(2) Figure C.2.1-2 shows the flowchart when message IDs described in Table C.2.1-2 are output due to the failure of new installation.

Table C.2.1-2 Message IDs List (2)

Message ID	KAQG61020-E KAQG61021-E KAQG61022-E KAQG61009-E KAQG61011-E KAQG61012-E KAQG61013-E KAQG61014-E KAQG61015-E KAQM01024-E KAQM01025-E KAQM01026-E KAQM01028-E KAQM01097-E KAQM14105-E KAQM14134-E KAQM14150-E KAQM14152-E

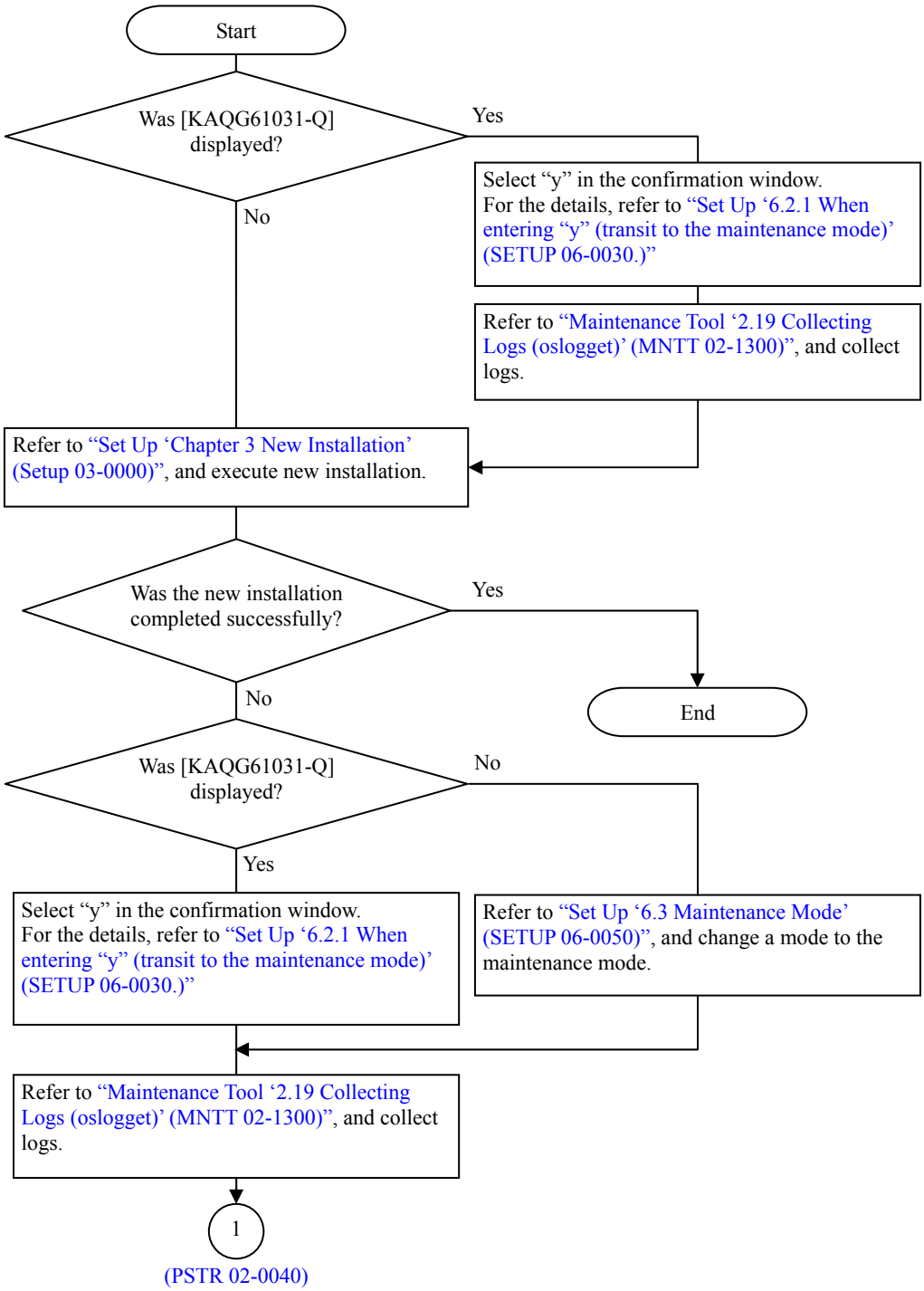
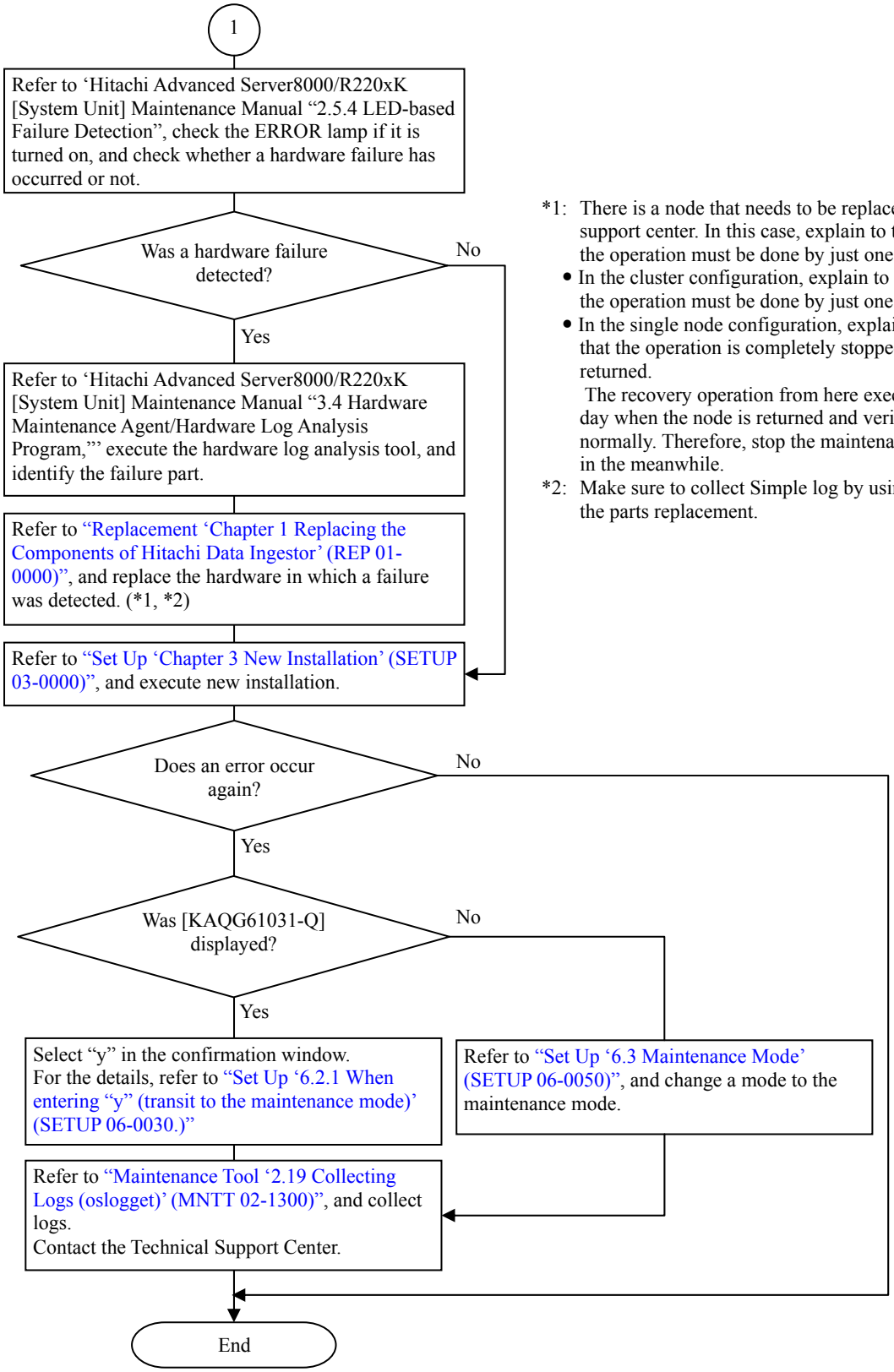


Figure C.2.1-2 Flow of Diagnosis for New Installation Failures (1/2)

Copyright © 2011, 2013, Hitachi, Ltd.



*1: There is a node that needs to be replaced the parts at the support center. In this case, explain to the customer that the operation must be done by just one side node.
- In the cluster configuration, explain to the customer that the operation must be done by just one side node.
- In the single node configuration, explain to the customer that the operation is completely stopped until the node is returned.

  The recovery operation from here executes some other day when the node is returned and verified that it works normally. Therefore, stop the maintenance operation here in the meanwhile.

*2: Make sure to collect Simple log by using HATP before the parts replacement.

Figure C.2.1-2 Flow of Diagnosis for New Installation Failures (2/2)

Copyright © 2011, 2014, Hitachi, Ltd.

(3) Figure C.2.1-3 shows the flowchart when message IDs described in Table C.2.1-3 are output due to the failure of update installation.

Table C.2.1-3 Message IDs List (3)

Message ID	KAQG61009-E KAQG61020-E KAQG61021-E KAQG61022-E KAQG61011-E KAQG61012-E KAQG61013-E KAQG61014-E KAQG61015-E KAQG61016-E KAQM01024-E KAQM01025-E KAQM01026-E KAQM01028-E KAQM01097-E KAQM14105-E KAQM14134-E KAQM14150-E KAQM14152-E

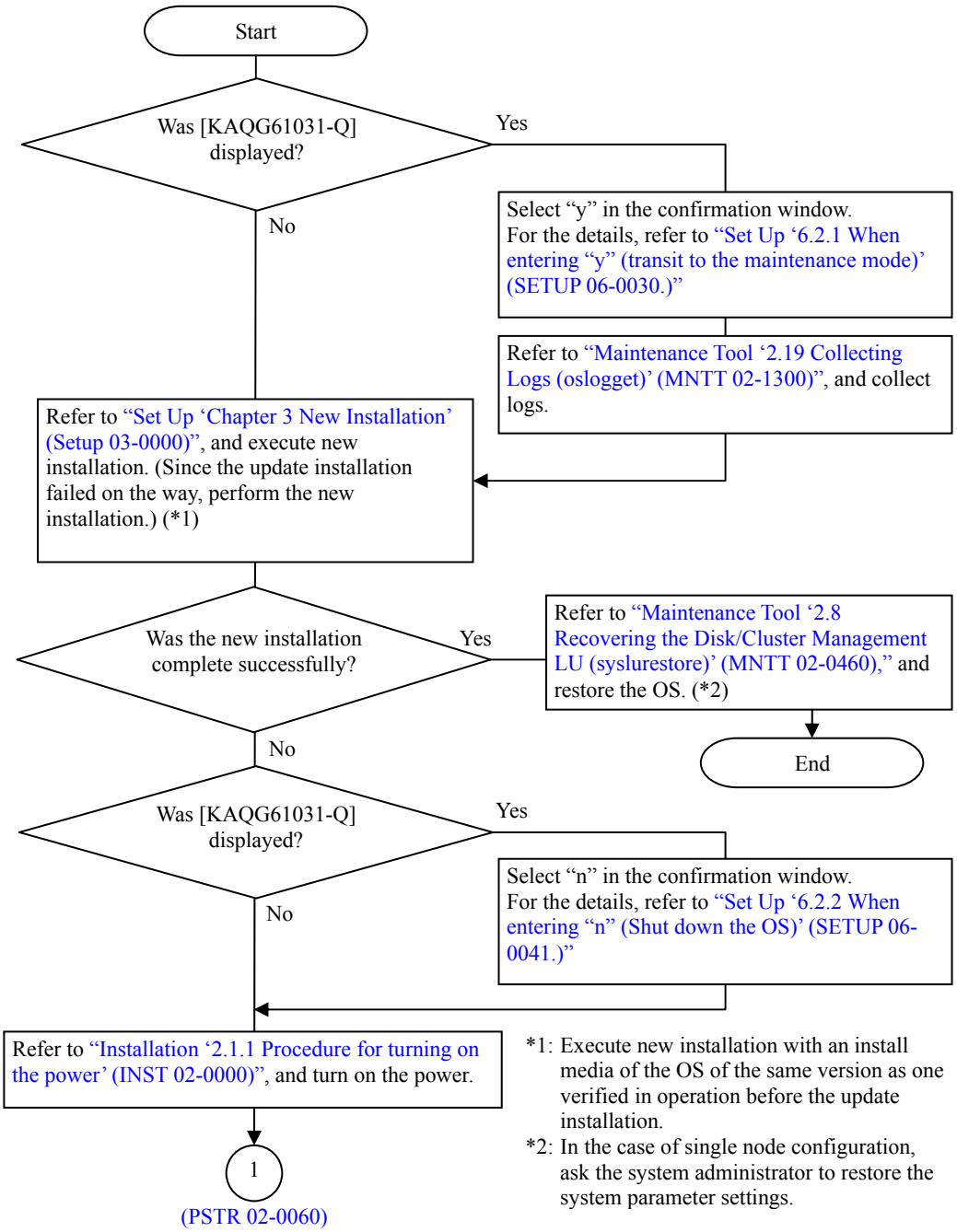


Figure C.2.1-3 Flow of Diagnosis for Update Installation Failures (1/4)

Copyright © 2011, 2015, Hitachi, Ltd.

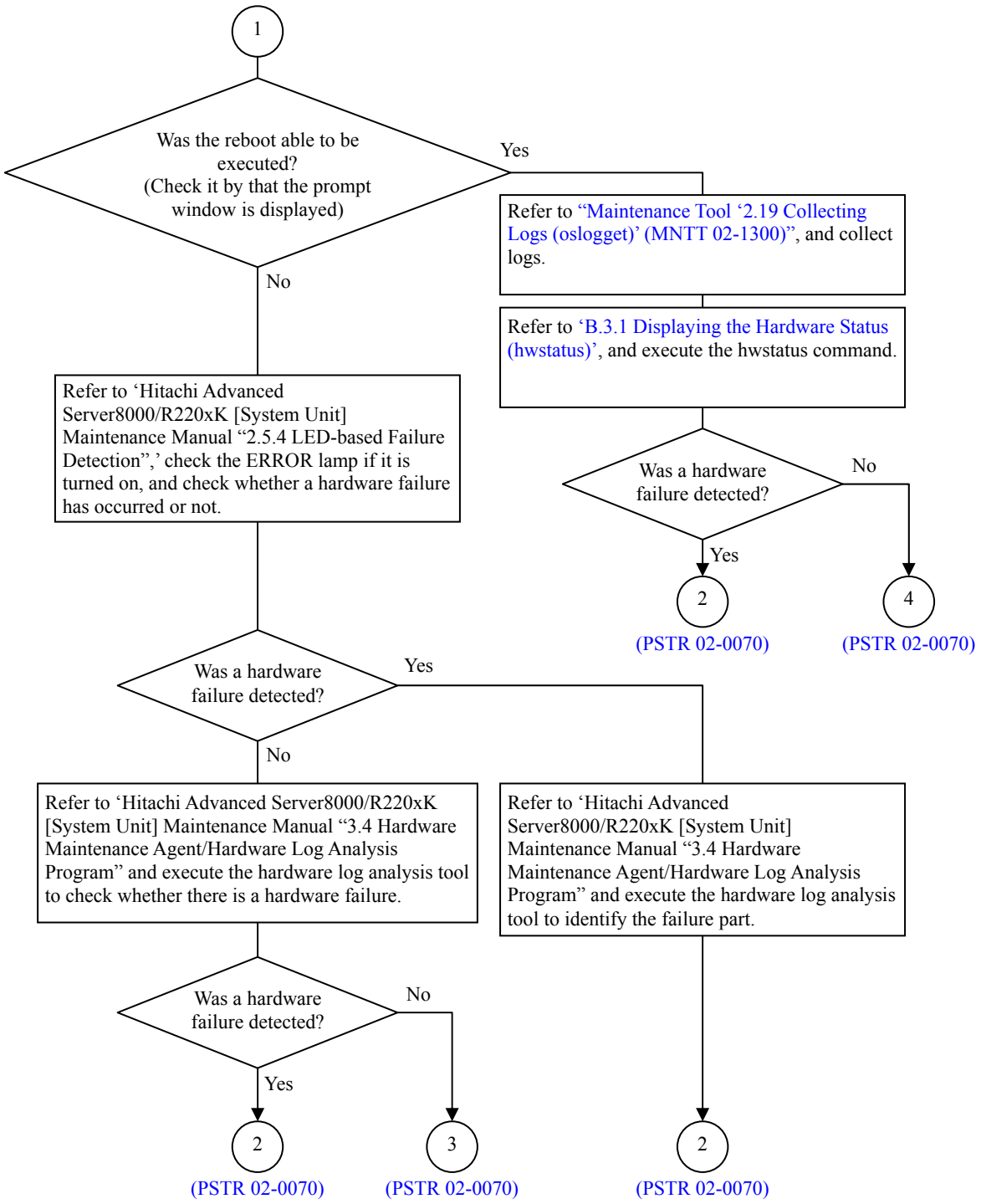
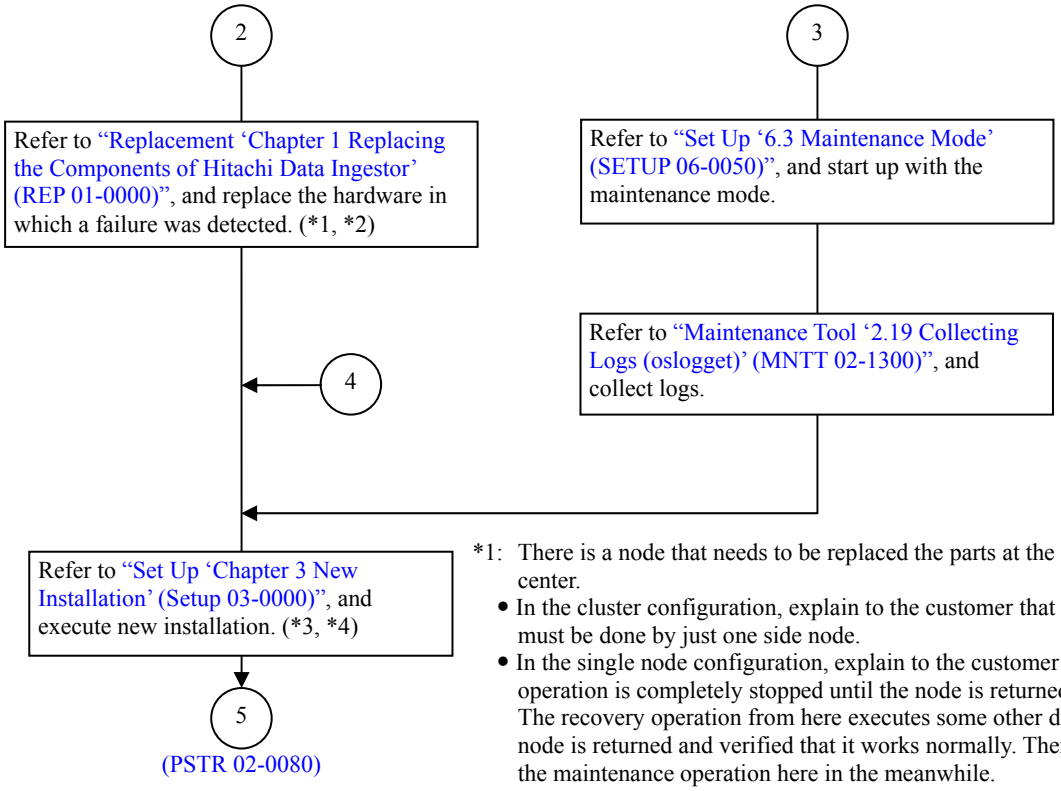


Figure C.2.1-3 Flow of Diagnosis for Update Installation Failures (2/4)

Copyright © 2011, 2013, Hitachi, Ltd.



*1: There is a node that needs to be replaced the parts at the support center.
- In the cluster configuration, explain to the customer that the operation must be done by just one side node.
- In the single node configuration, explain to the customer that the operation is completely stopped until the node is returned.
  The recovery operation from here executes some other day when the node is returned and verified that it works normally. Therefore, stop the maintenance operation here in the meanwhile.

*2: Make sure to collect Simple log by using HATP before the parts replacement.

*3: In the single node configuration (in the case of Configuration using trunk 2 Data ports), request the system administrator if there is unoccupied port in the IP-SW that is configured by the customer. And then connect with the LAN cable between the unoccupied port and the management port of the node.

*4: Execute new installation with an install media of the OS of the same version as one verified in operation before the update installation.

Figure C.2.1-3 Flow of Diagnosis for Update Installation Failures (3/4)

Copyright © 2011, 2014, Hitachi, Ltd.

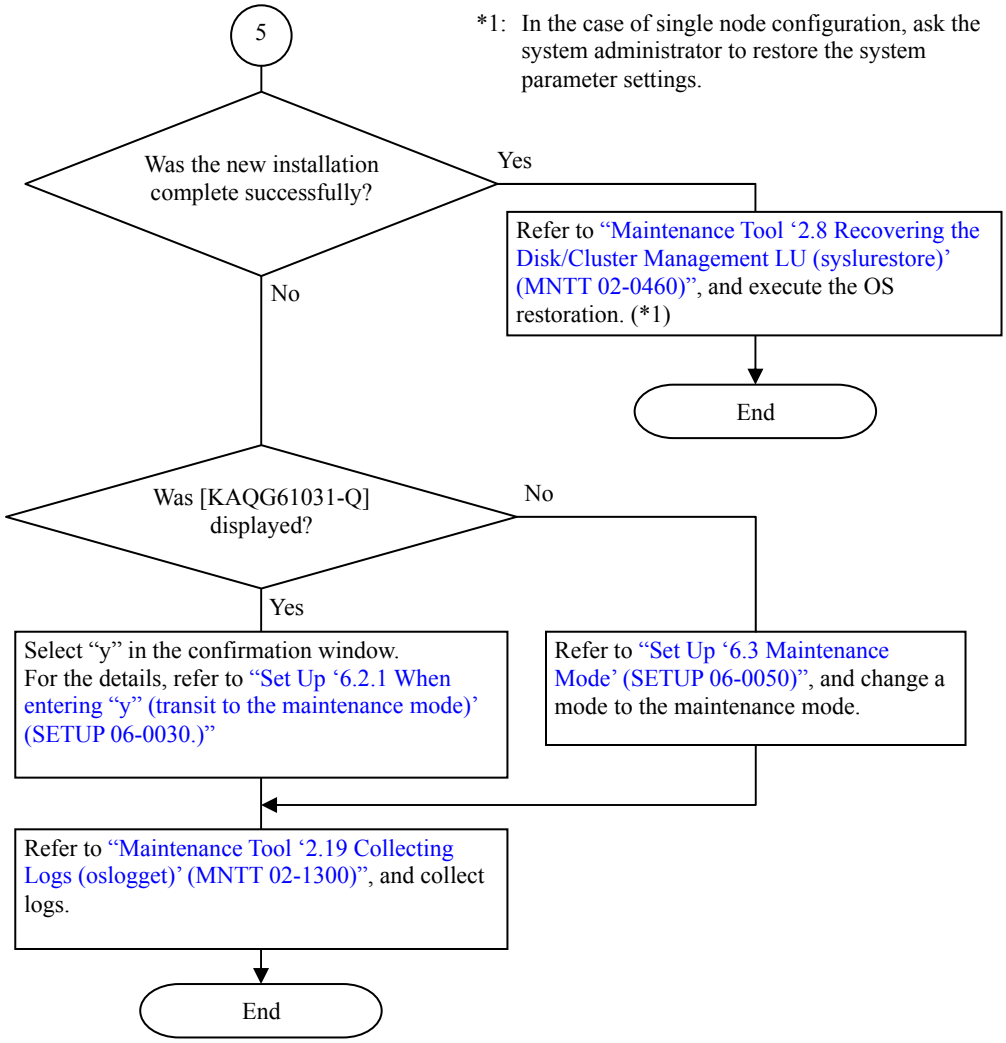


Figure C.2.1-3 Flow of Diagnosis for Update Installation Failures (4/4)

Copyright © 2011, 2013, Hitachi, Ltd.

(4) Figure C.2.1-4 shows the flowchart when message IDs described in Table C.2.1-4 are output due to the failure of update installation.

Table C.2.1-4 Message ID List (4)

Message ID	KAQG61018-W

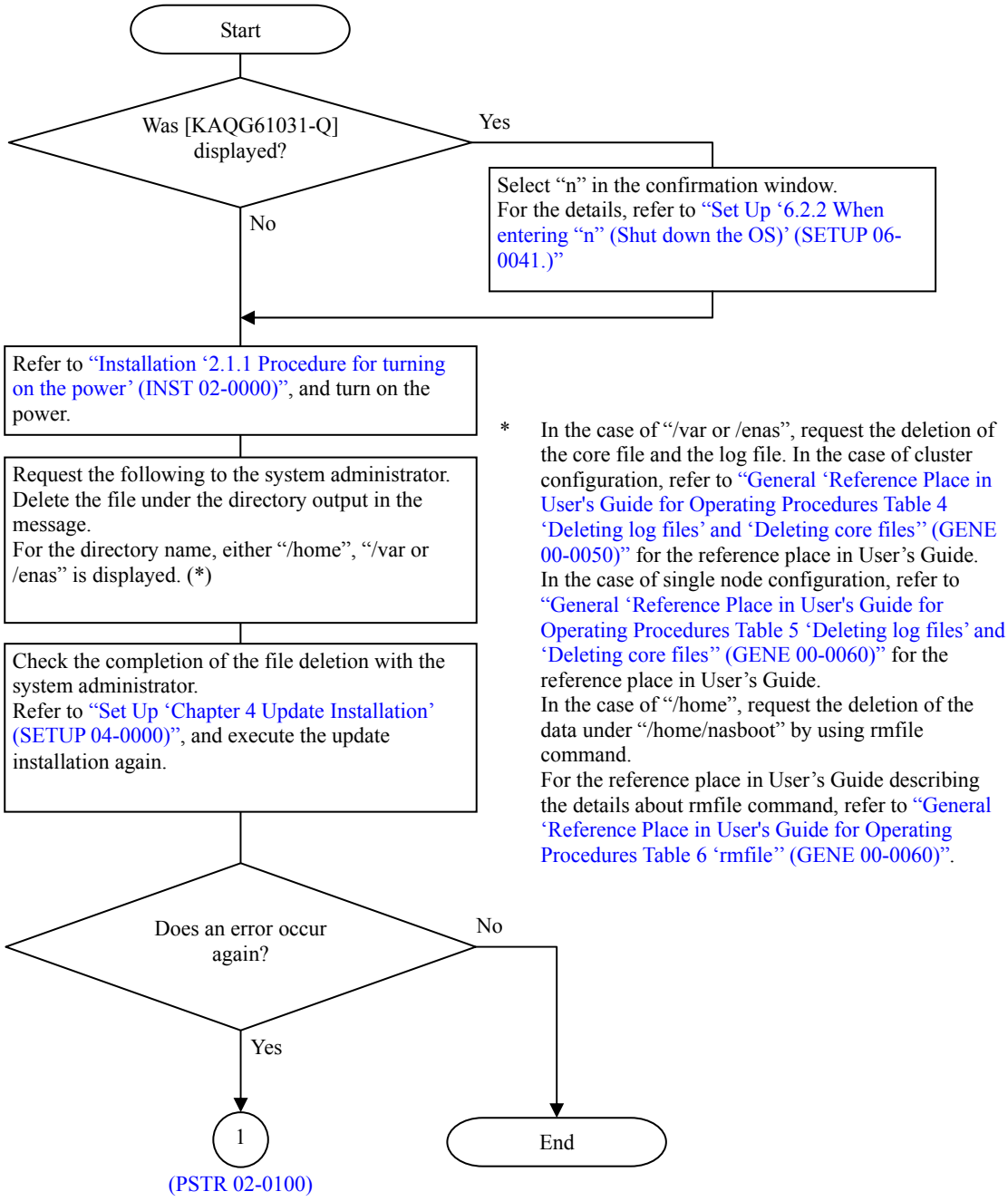


Figure C.2.1-4 Flow of Diagnosis for Lack of Free Space (1/2)

Copyright © 2011, 2013, Hitachi, Ltd.

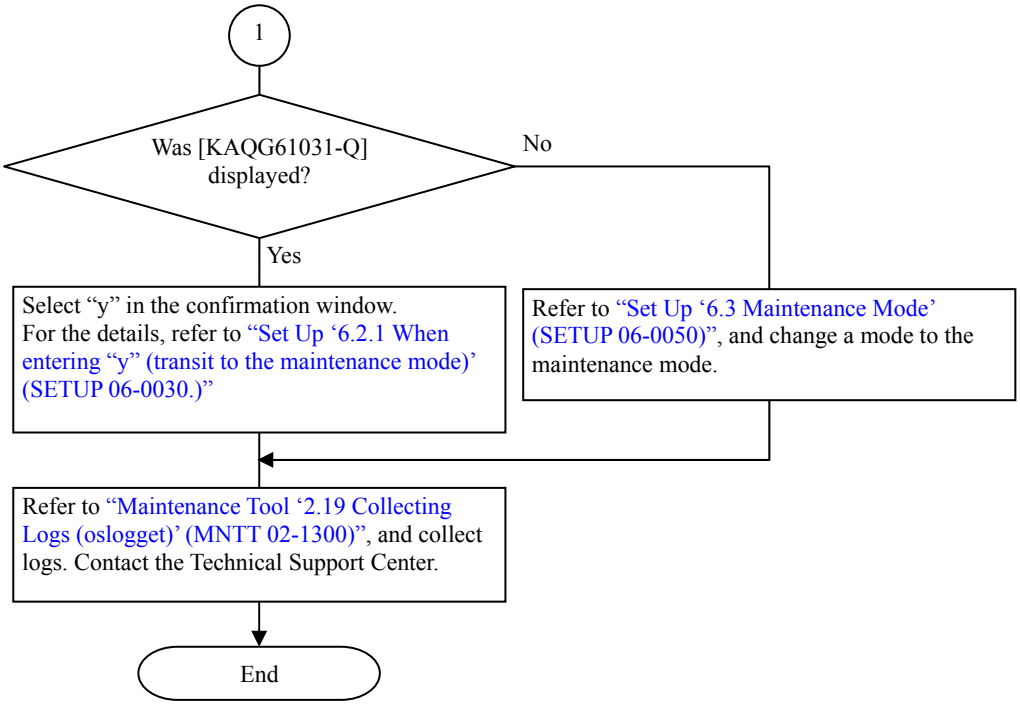


Figure C.2.1-4 Flow of Diagnosis for Lack of Free Space (2/2)

Copyright © 2011, 2013, Hitachi, Ltd.

(5) Figure C.2.1-5 shows the flowchart when message IDs described in Table C.2.1-5 are output by the version check during update installation.

Table C.2.1-5 Message ID List (5)

Message ID	KAQG61024-E

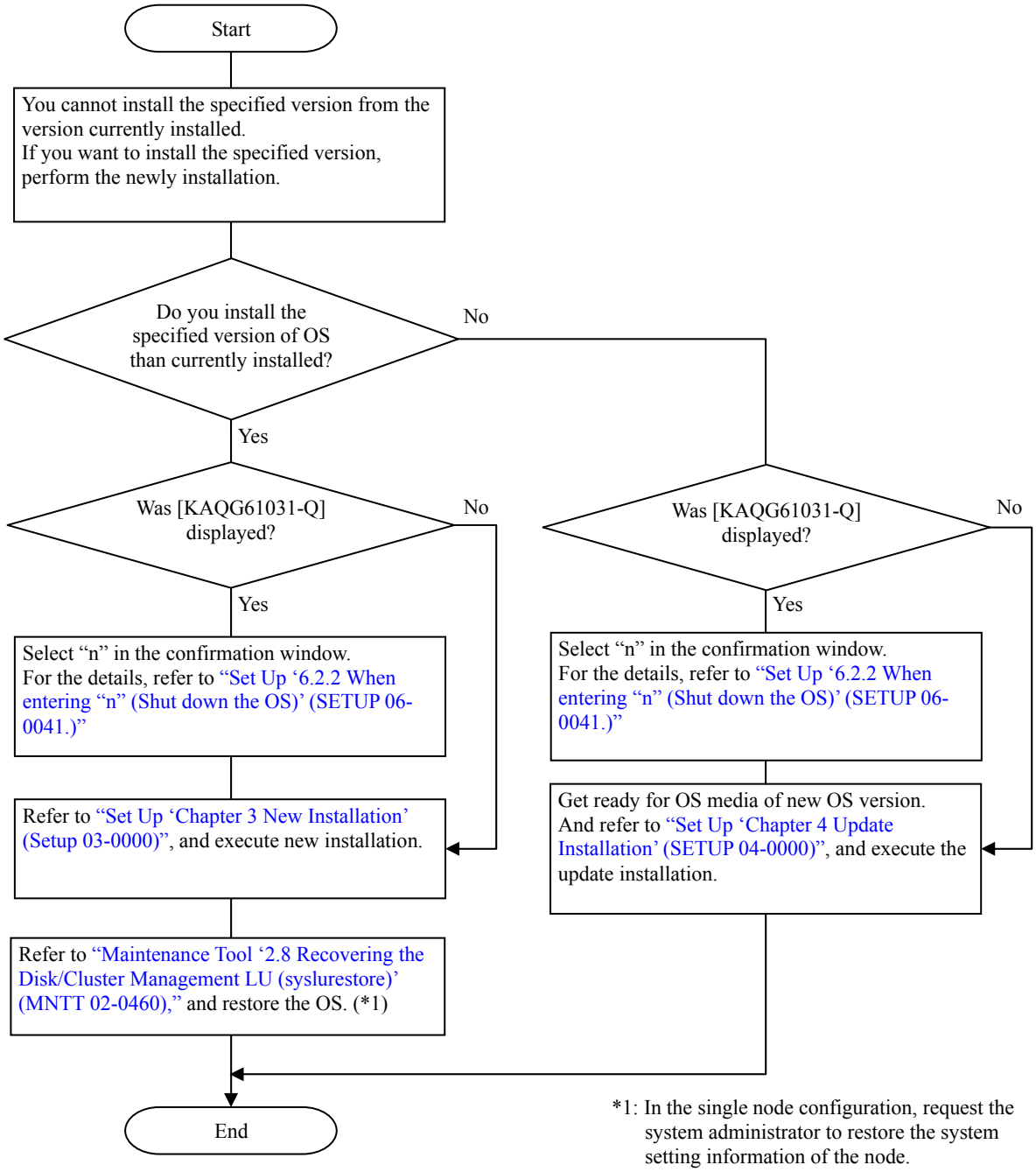


Figure C.2.1-5 Flow of Diagnosis when Checking the Version during Update Installation

Copyright © 2011, 2015, Hitachi, Ltd.

(6) Figure C.2.1-6 shows the flowchart when message IDs described in Table C.2.1-6 are output because the update installation is executed in the state of no OS installed.

Table C.2.1-6 Message ID List (6)

Message ID	KAQG61028-E

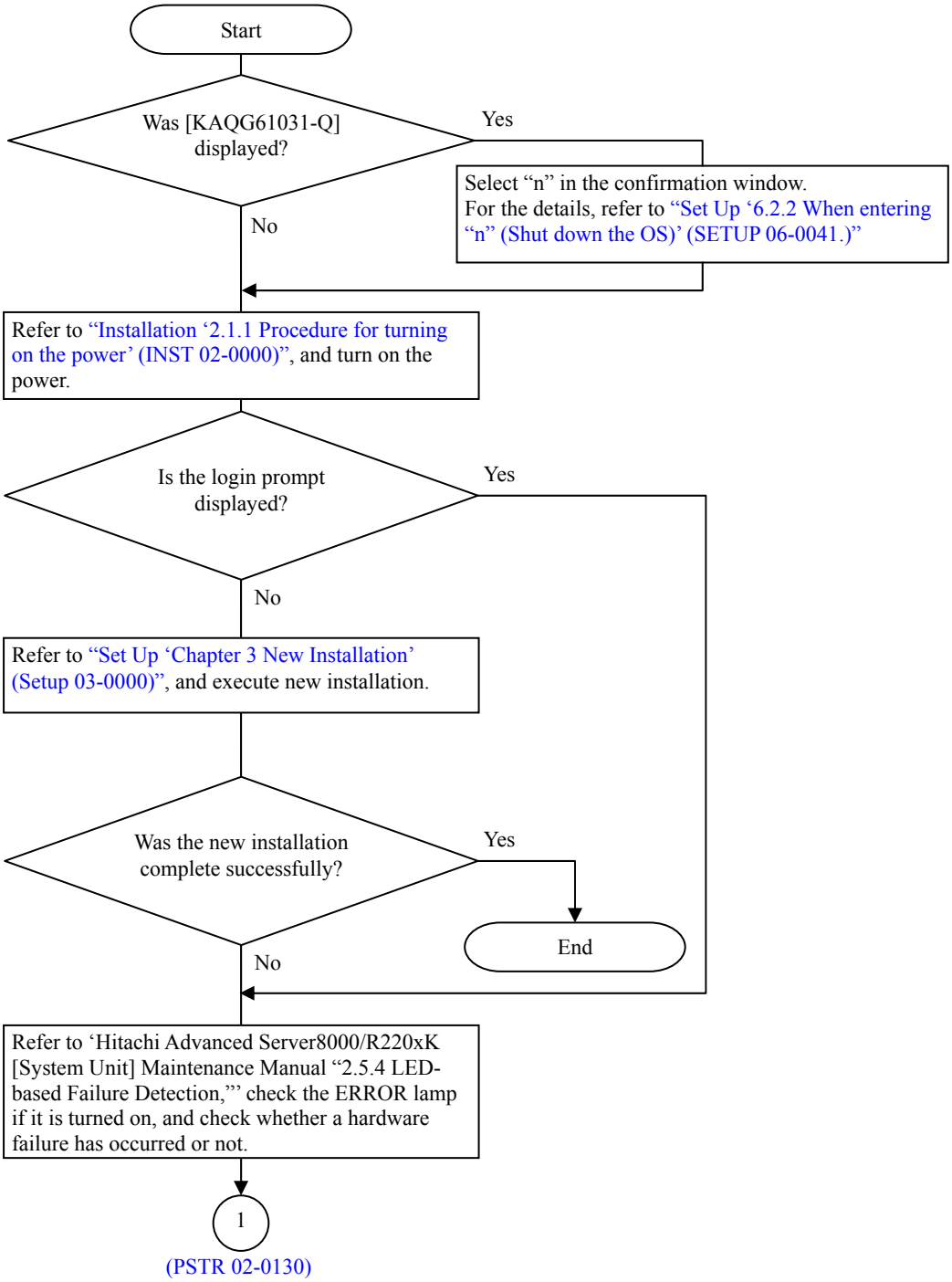
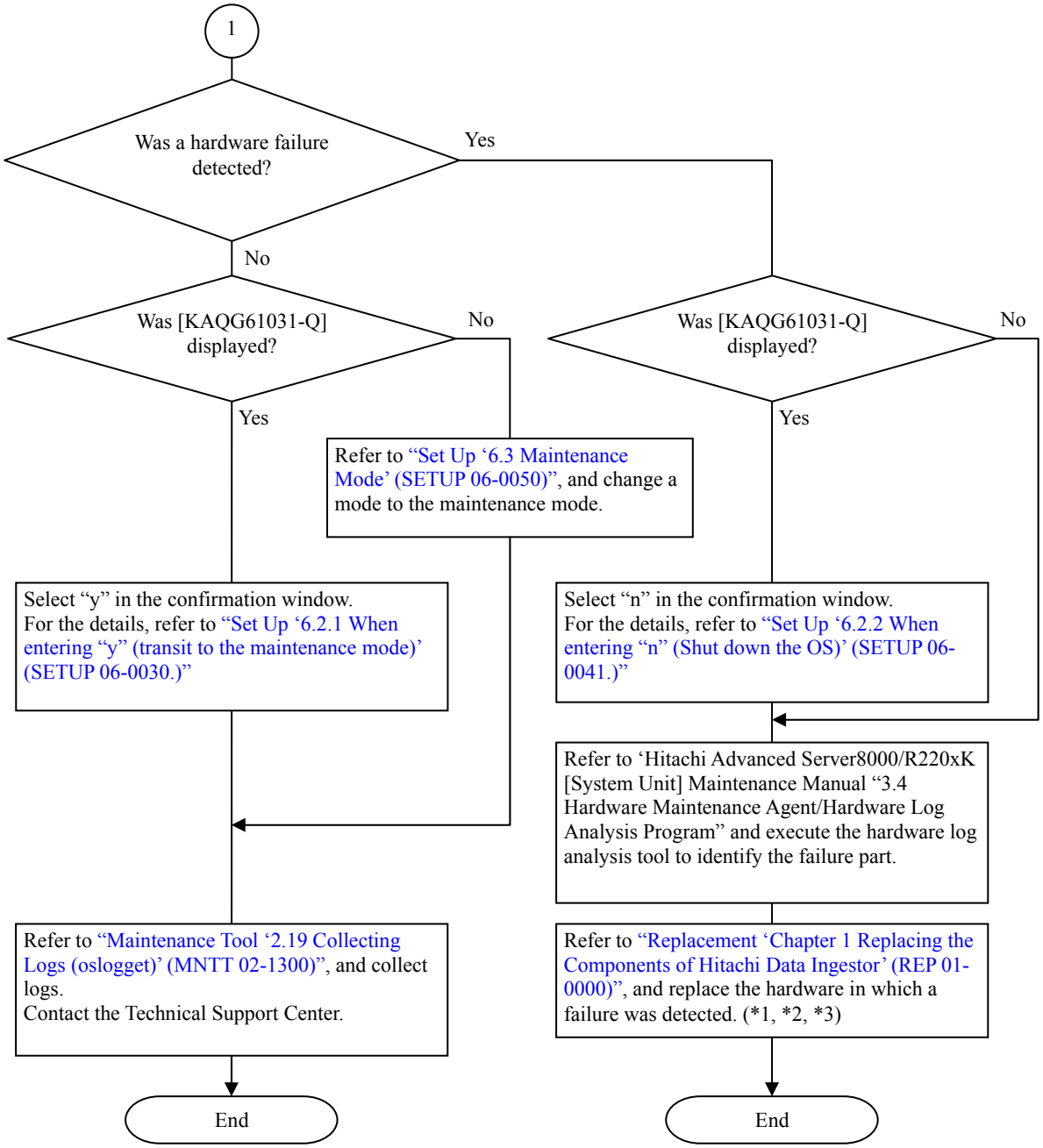


Figure C.2.1-6 Flow of Diagnosis when the Update Installation Failed (1/2)

Copyright © 2011, 2014, Hitachi, Ltd.



*1: Make sure to collect Simple log by using HATP before the parts replacement.

*2: There is a node that needs to be replaced the parts at the support center.

- In the cluster configuration, explain to the customer that the operation must be done by just one side node.
- In the single node configuration, explain to the customer that the operation is completely stopped until the node is returned.

  The recovery operation from here executes some other day when the node is returned and verified that it works normally. Therefore, stop the maintenance operation here in the meanwhile.

*3: If the new installation is executed along with the parts replacement, use an install media of the OS of the same version as one verified in operation before the update installation to execute the installation.

Figure C.2.1-6 Flow of Diagnosis when the Update Installation Failed (2/2)

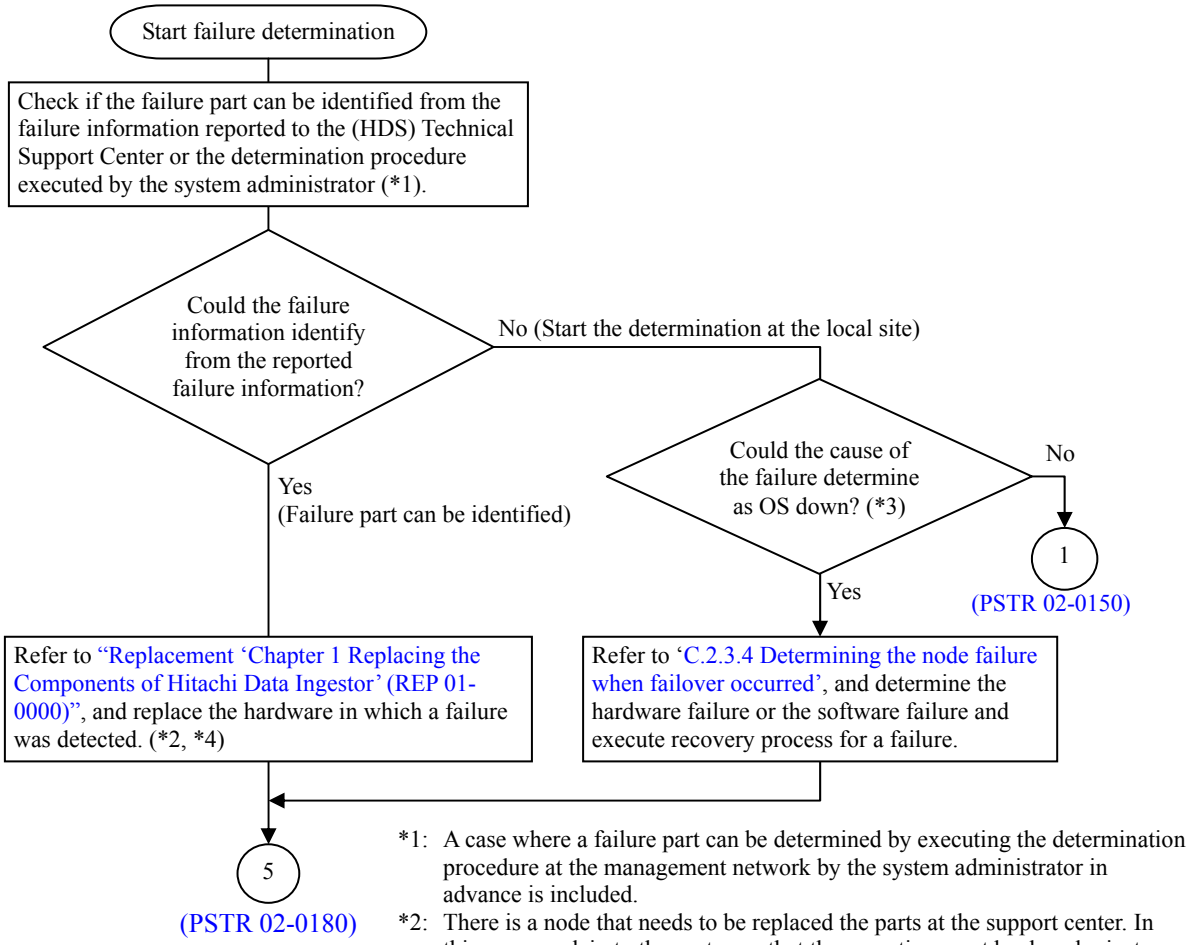
Copyright © 2011, 2014, Hitachi, Ltd.

C.2.2 Determination Procedure when a Failure Occurred

C.2.2.1 Failure determination procedure at the cluster configuration

After checking the power supply and the management system network, the failure is determined to either a hardware system failure or a software system failure depending on whether SIM of failover is acquired or not. The entire flow of the failure determination is shown below.

NOTE:
- If the OS version 5.1.0-XX and later, and File Version Restore Function is used, “data of the past version directory” might be inaccessible for a moment after performing failover or failback. Contact the system administrator when failover or failback is to be performed.
- If the logical failure is occured on the file system using Active File Migration or Large file transfer, the maintenance personnel might not be able to identify the failure location with the failure determination procedure. Before the completion maintenance procedure, inform system administrator that they can start recovering the work space for AFM.



*1: A case where a failure part can be determined by executing the determination procedure at the management network by the system administrator in advance is included.

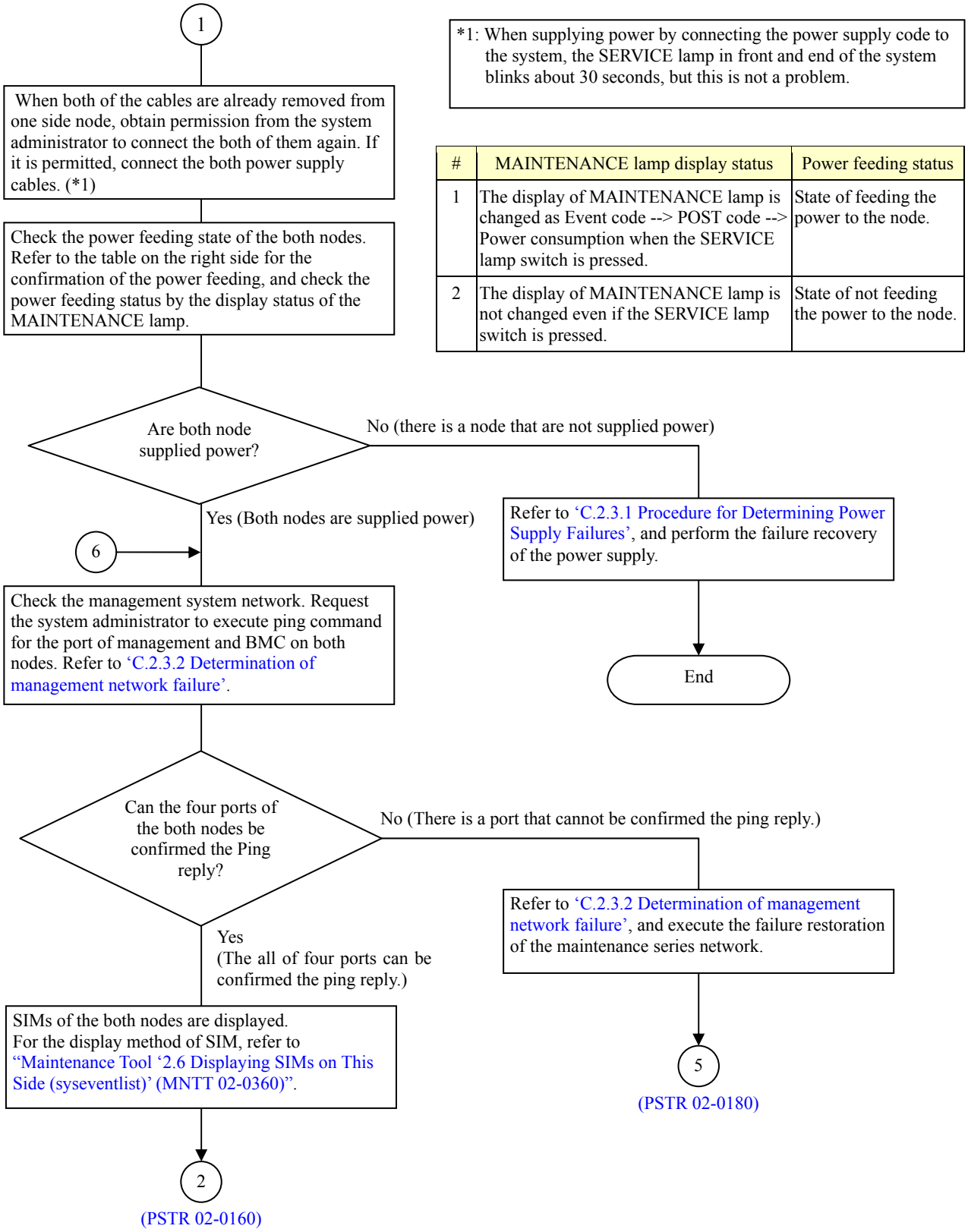
*2: There is a node that needs to be replaced the parts at the support center. In this case, explain to the customer that the operation must be done by just one side node. The recovery operation from here executes some other day when the node is returned and verified that it works normally. Therefore, stop the maintenance operation here in the meanwhile.

*3: This is only for the case when it could not communicate with the management port of one side node and confirmed as OS down by executing the determination procedure at the management network by the system administrator in advance.

*4: Make sure to collect Simple log by using HATP before the parts replacement.

Figure C.2.2.1-1 Procedure for determining failures (1/5)

Copyright © 2011, 2017, Hitachi, Ltd.



*1: When supplying power by connecting the power supply code to the system, the SERVICE lamp in front and end of the system blinks about 30 seconds, but this is not a problem.

#	MAINTENANCE lamp display status	Power feeding status
1	The display of MAINTENANCE lamp is changed as Event code --> POST code --> Power consumption when the SERVICE lamp switch is pressed.	State of feeding the power to the node.
2	The display of MAINTENANCE lamp is not changed even if the SERVICE lamp switch is pressed.	State of not feeding the power to the node.

Figure C.2.2.1-1 Procedure for determining failures (2/5)

Copyright © 2011, 2013, Hitachi, Ltd.

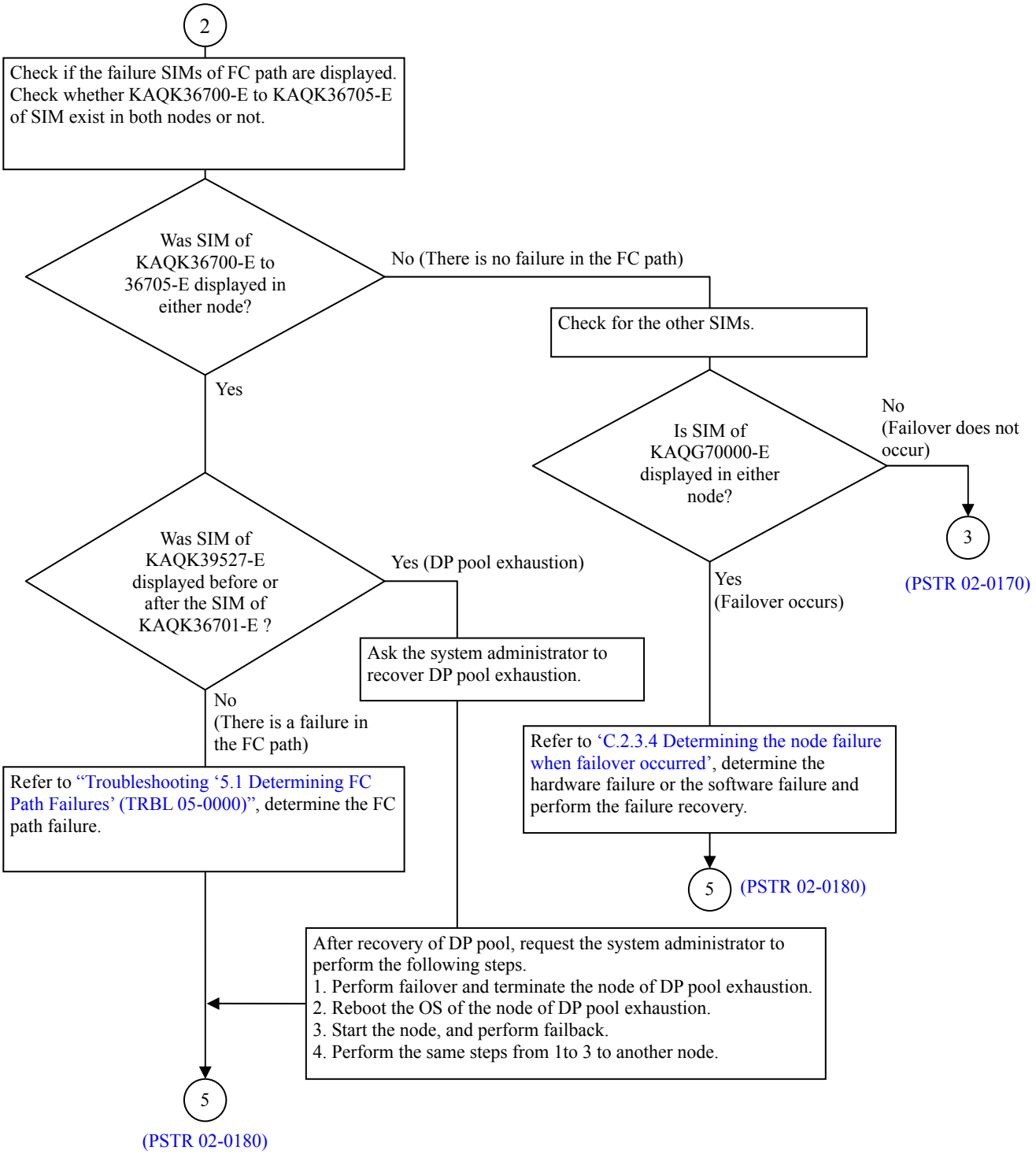


Figure C.2.2.1-1 Procedure for determining failures (3/5)

Copyright © 2011, 2013, Hitachi, Ltd.

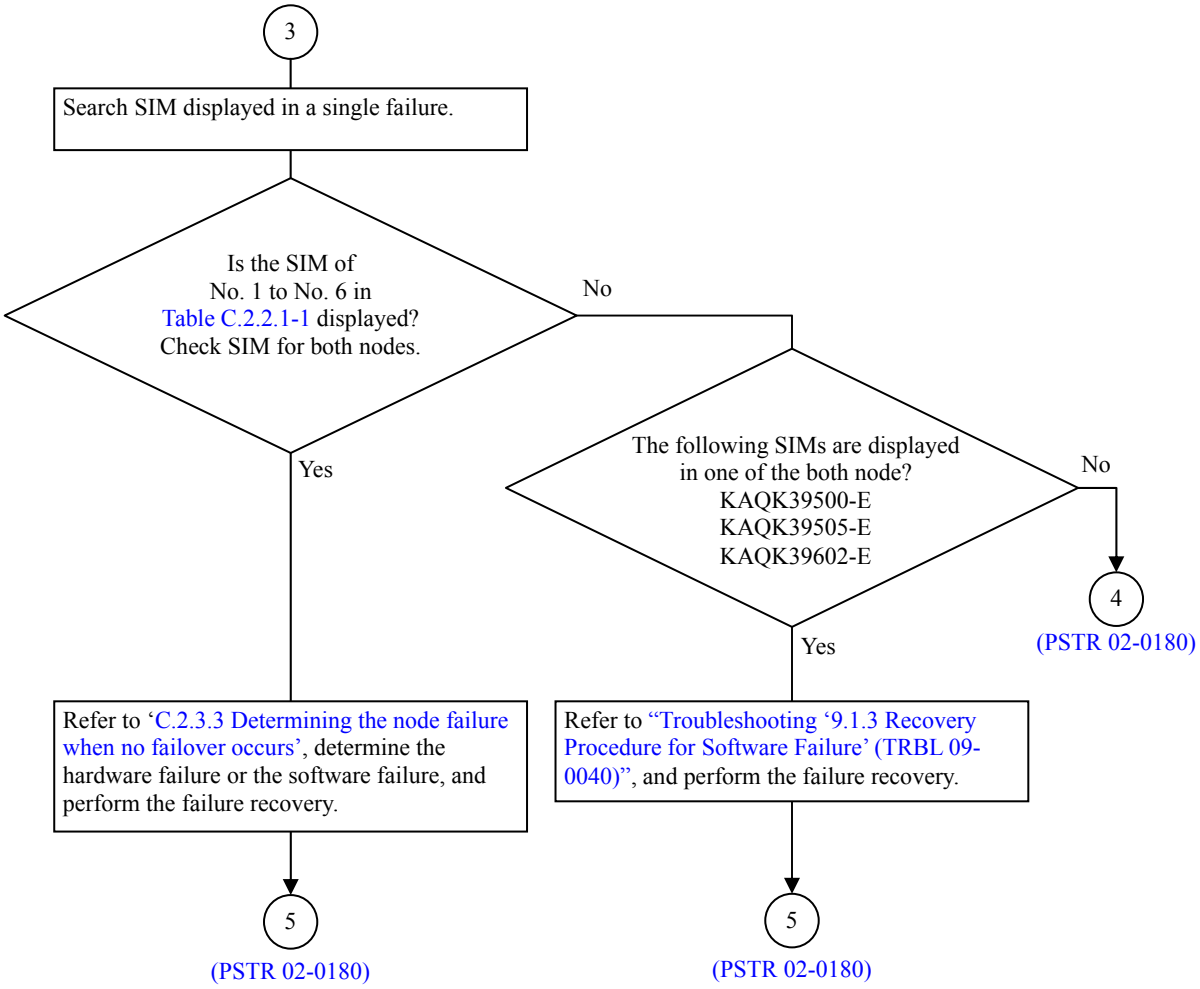


Figure C.2.2.1-1 Procedure for determining failures (4/5)

Copyright © 2011, 2013, Hitachi, Ltd.

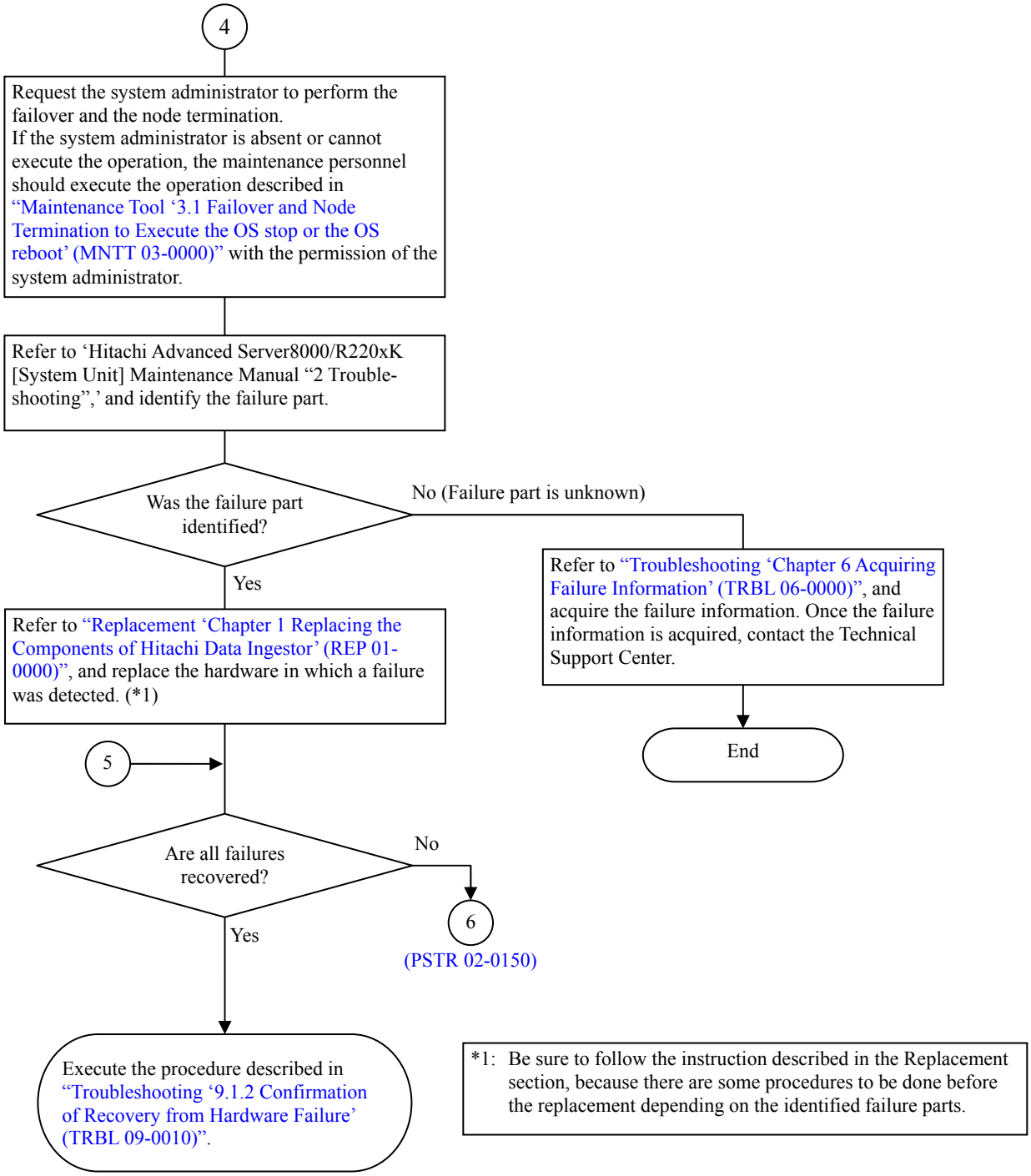


Figure C.2.2.1-1 Procedure for determining failures (5/5)

Copyright © 2011, 2013, Hitachi, Ltd.

Table C.2.2.1-1 Failed parts shown by SIM

#	SIM	Lamp status	Checking the status by the hwstatus command (*1)	Failed part
1	KAQG72012-W	—	Is the Heartbeat LAN port status “Link down”?	Heartbeat LAN port or Heartbeat LAN cable (*2) (*3)
2	KAQG81003-W	—	Is the port status “Link down”?	Extension NIC port or cable (*2) (*3)
3	KAQK30801-E	—	—	Identify the failure part from the RC and continuous log that are described in the SIM. (*4)
4	KAQK39504-E	—	Is the status of all ports of NIC “Link down”?	—
5	KAQK39538-E	—	—	Virtual Server that has Virtual Server ID displayed in a message.
6	KAQK39527-E	—	—	Pool exhaustion (*5)

*1: For the hwstatus command, refer to ‘B.3.1 Displaying the Hardware Status (hwstatus)’.
*2: When it is not recovered even if the cable is replaced, it is a port failure.
*3: In case of a port failure, ping from the management PC or maintenance PC, and specify which of the nodes has the port failure.
*4: For identifying a failure part from the RC and the continuous log, refer to “Hitachi Advanced Server8000/RS220xK [System Unit] Maintenance Manual”.
*5: Ask the system administrator to recover the pool exhaustion.

Copyright © 2011, 2016, Hitachi, Ltd.

C.2.2.2 Failure determination procedure at the single node configuration

In the single node configuration, a failure is determined to either a hardware system failure or a software system failure after checking the power supply and FC path failure SIM. The entire flow of the failure determination is shown below.

NOTE:
- Because there are two configurations in the single node configuration, make sure the target configuration before the operation. For the configuration, refer to "Installation '1.1.4 Overall configuration diagram (1-2) Single node configuration (when not using the disk array subsystem)' (INST 01-0072B)", "Installation '1.1.4 Overall configuration diagram (1-3) Single node configuration (when using the disk array subsystem)' (INST 01-0072C)", or "Installation '1.1.4 Overall configuration diagram (4) Overall system configuration diagram in the configuration of HDI for Cloud (single node)' (INST 01-0078)".
- If the OS version 5.1.0-XX and later, and File Snapshots Function or File Version Restore Function is used, "differential-data snapshot" or "data of the past version directory" might be inaccessible for a moment after the start-up of the resource groups. Contact the system administrator when the resource groups are to be started or restarted.
- If the logical failure is occured on the file system using Active File Migration or Large file transfer, the maintenance personnel might not be able to identify the failure location with the failure determination procedure. Before the completion maintenance procedure, inform system administrator that they can start recovering the work space for AFM.

Copyright © 2011, 2017, Hitachi, Ltd.

#	MAINTENANCE lamp display status	Power Feeding Status
1	The display of MAINTENANCE lamp is changed as Event code --> POST code --> Power consumption in each time the SERVICE lamp switch is pressed.	State of feeding the power to the node.
2	The display of MAINTENANCE lamp is not changed even if the SERVICE lamp switch is pressed.	State of not feeding the power to the node.

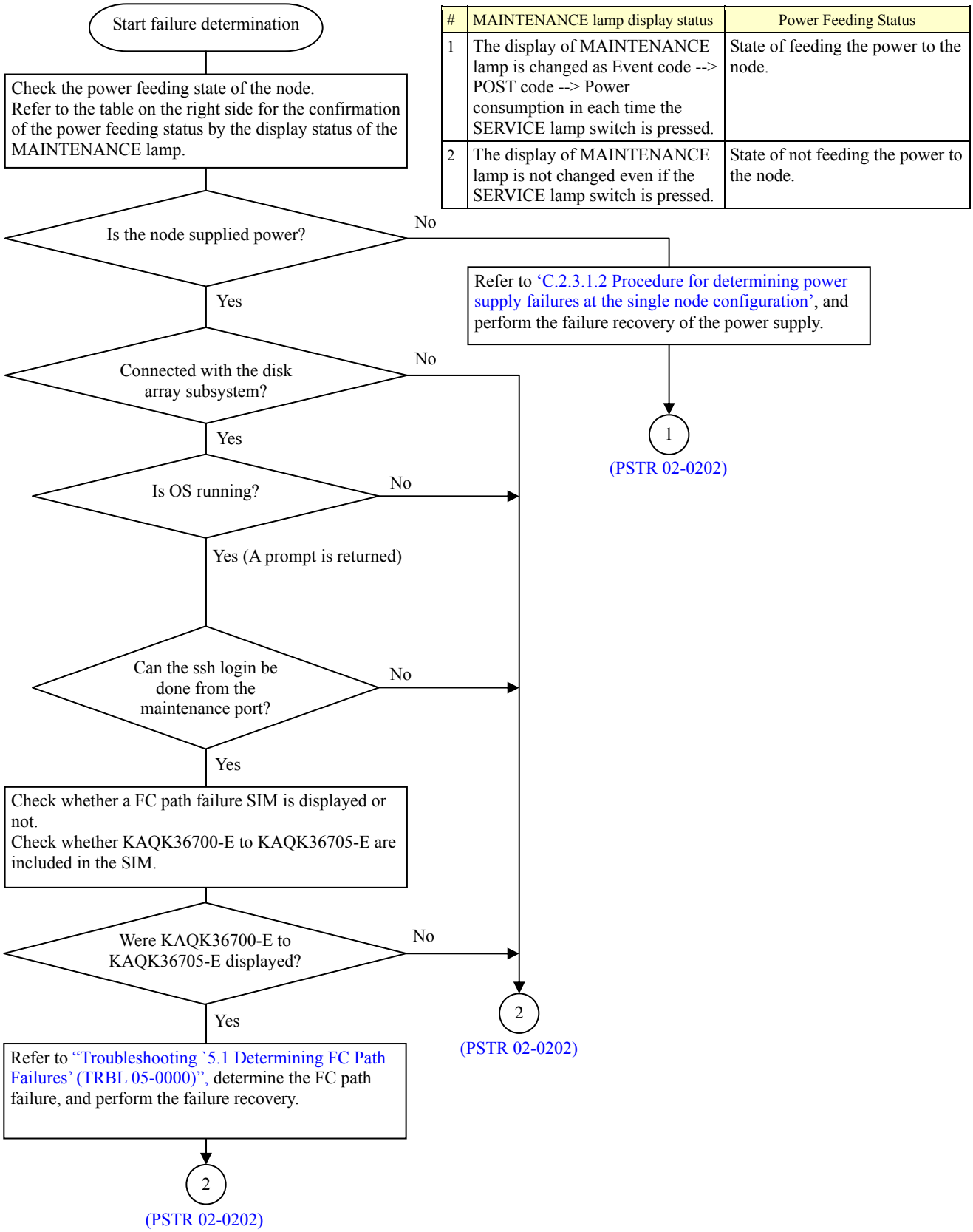


Figure C.2.2.2-1 Failure determination process at the single node configuration (1/2)

Copyright © 2012, 2013, Hitachi, Ltd.

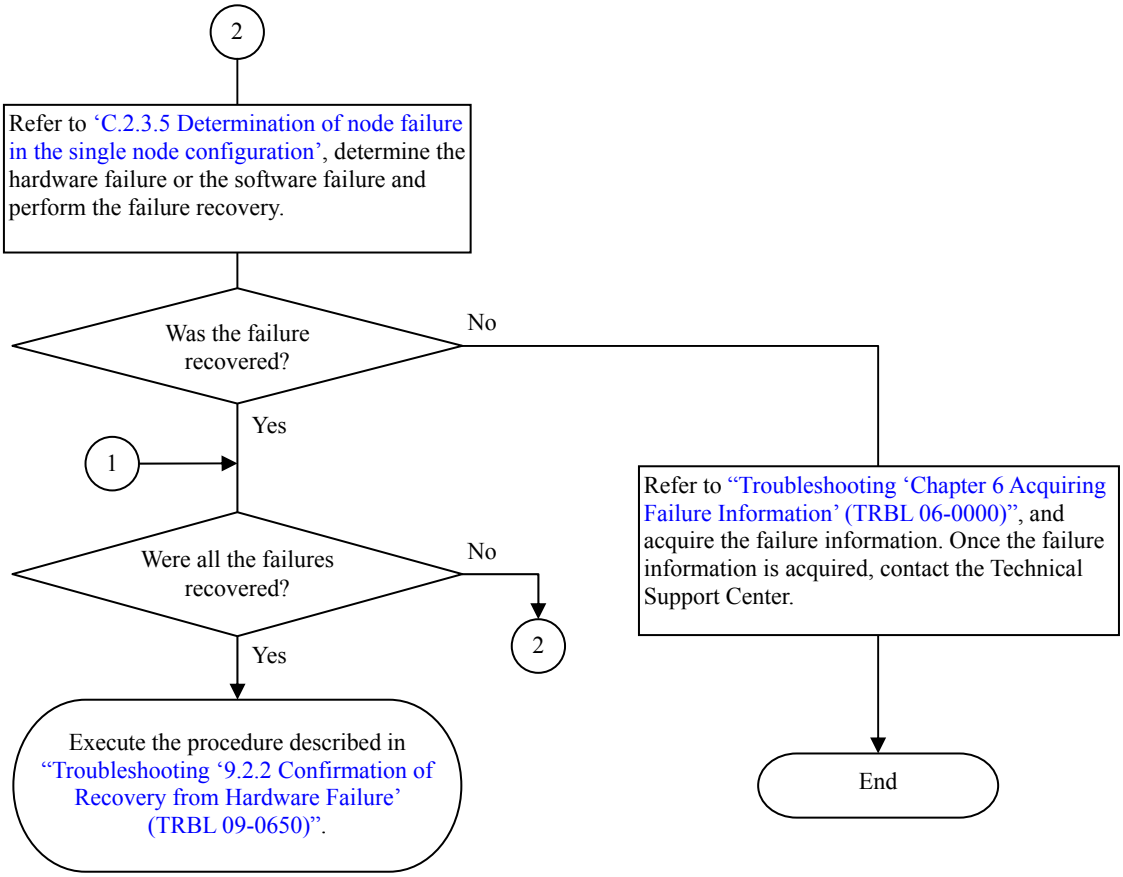


Figure C.2.2.2-1 Failure determination process at the single node configuration (2/2)

Copyright © 2012, 2013, Hitachi, Ltd.

C.2.3 Detailed Determination Procedure in Each Failure

C.2.3.1 Procedure for determining power supply failures

C.2.3.1.1 Procedure for determining power supply failures in the cluster configuration

The procedure for determining power supply failures is shown in the following flow.
It is assumed that, for one side node, at least one side power supply lamp does not light up or lights up in amber, or the distribution board failure occurred.

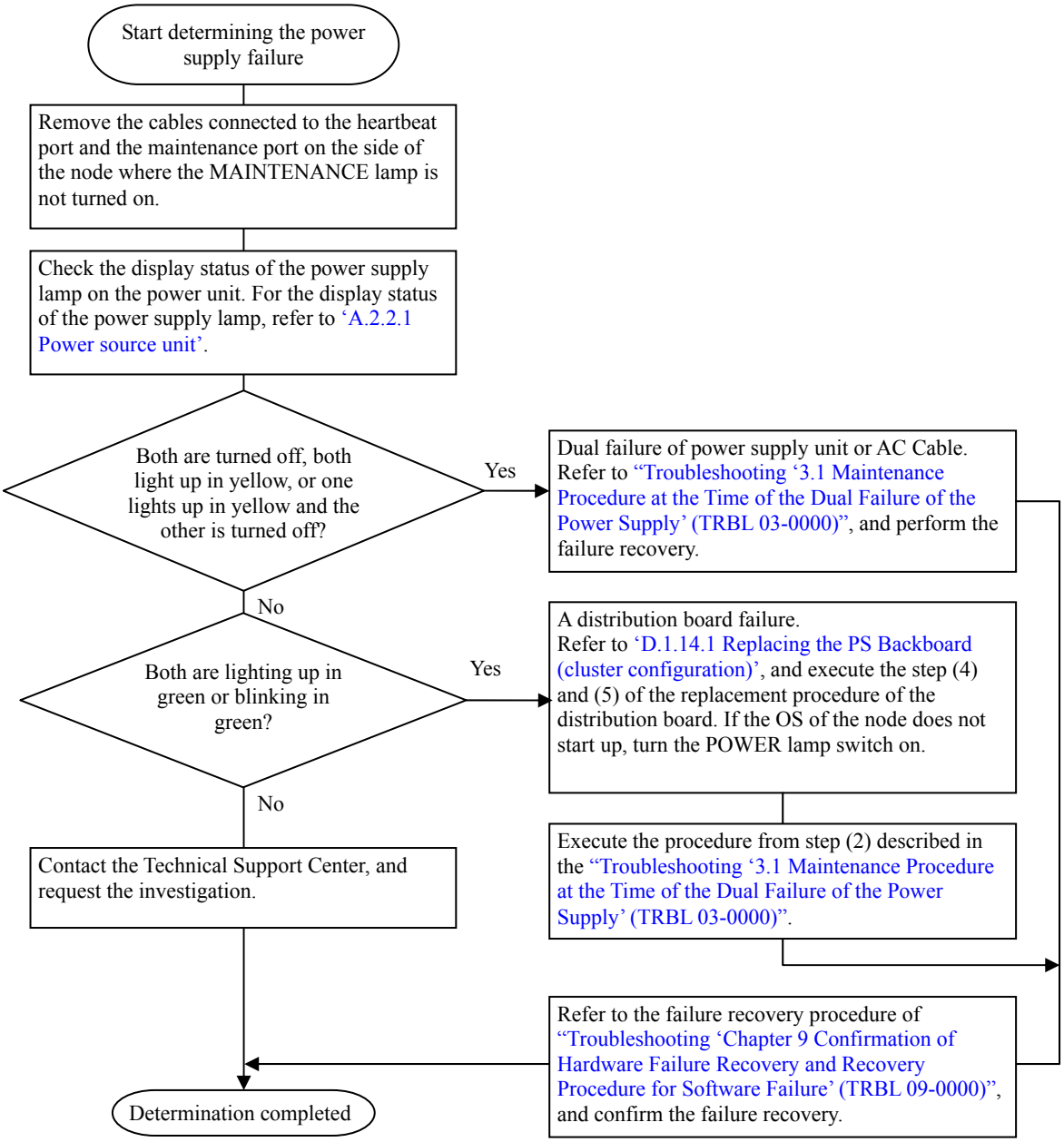


Figure C.2.3.1.1-1 Procedure for determining power supply failures

Copyright © 2011, 2013, Hitachi, Ltd.

C.2.3.1.2 Procedure for determining power supply failures at the single node configuration

The following flowchart shows the procedure of power supply failures. It is assumed that the power supply lamp does not turn on, blinking in amber light, or a distribution board failure occurred.

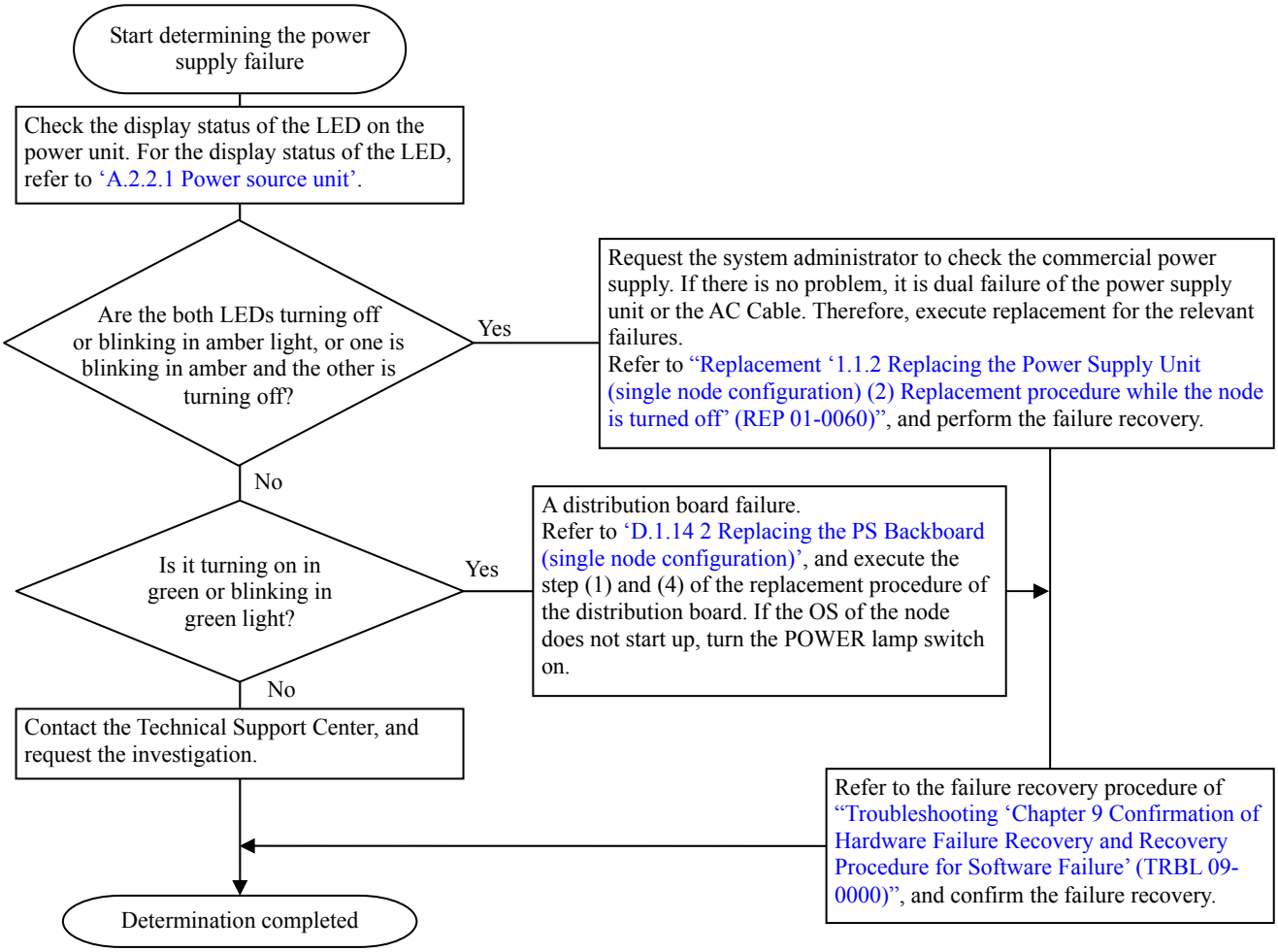


Figure C.2.3.1.2-1 Procedure for determining power supply failures

Copyright © 2011, 2013, Hitachi, Ltd.

C.2.3.2 Determination of management network failure

This chapter describes determination of the management network failure.

When the failure location can be identified from the failure notice, maintenance personnel should perform the recovery operation for the relevant location.

When the failure location cannot be identified, determine the failed part by the determination operation described in this chapter, and then perform the recovery operation.

Check the following before performing the isolation of the failure.

Checking method varies depending on the model. However, confirm the status of the Power LED and the Status LED of IP-SW.

If the Power LED is “Off”, the power is turned off or a power failure. Check the power switch of the management LAN IP-SW, the power cable and the power to be supplied to the management LAN IP-SW. If the switch is not turned off and no problem with the power cable and the power supply, it is the IP-SW failure.

When the Status LED indicates an error, see the manual for the target product to perform the troubleshooting.

C.2.3.2.1 Failure determination by ping command execution result

Before performing the operation of management network failure determination, obtain the result (node0: mng0, BMC0 and node1: mng1, BMC1) of the ping command executed by the system administrator. Then, perform the determination operation.

Figure 4.1 Overview of Checking by Using ping Command shows an overview of the checking by using the ping command.

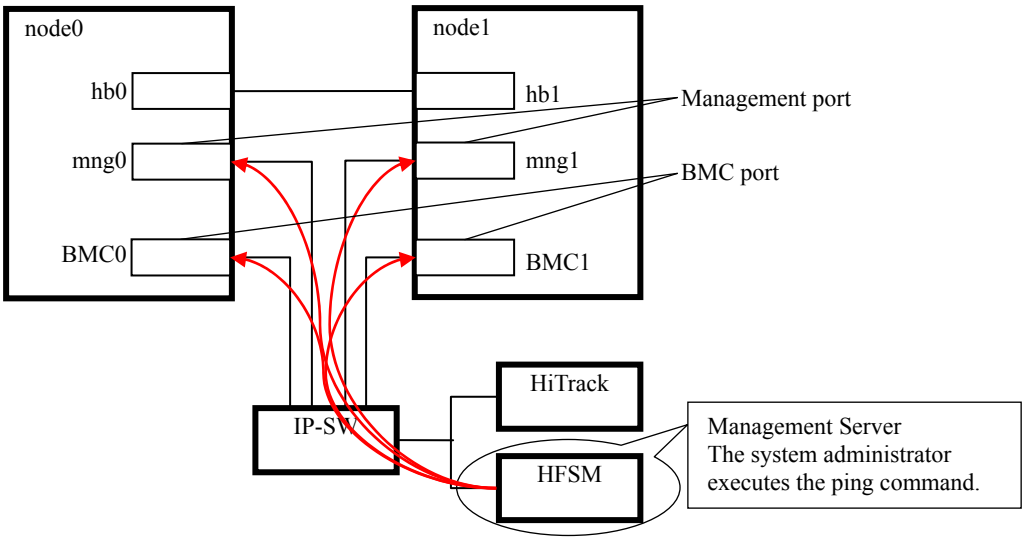


Figure C.2.3.2.1-1 Overview of Checking by Using ping Command

Based on the result of the ping command execution, determine the failure with reference to the ‘Table C.2.3.2.1-1 Matrix Table of Management Network Failures’.

Determination process is the same when the judgment of Yes/No in node0 and node1 are switched.

If there is no management network failure and the all results of the Y/N judgment for node 0 and node 1of each port shown in Table C.2.3.2.1-1 and Table C.2.3.2.1-2 are “Y”, return to the calling process.

Copyright © 2011, 2015, Hitachi, Ltd.

Table C.2.3.2.1-1 Matrix Table of Management Network Failures

#	Management port		BMC port		OS operation status	Resource group operation status (*4)	Assumed failure	Failure determination procedure
	node0	node1	node0	node1				
1	Y	Y	N	N	Both nodes are in operation	Operating in both nodes (Online/No error)	Double failures in the BMC ports or the cables occurred.	Execute the flow of Figure C.2.3.2.2-1. 'C.2.3.2.2 Flow of Management Network Failure Determination (1) Failure in the BMC ports or the cables'
2	Y	Y	Y	N	Both nodes are in operation	Operating in both nodes (Online/No error)	A failure in the BMC ports or the cables occurred.	
3	Y	N	Y	Y	Both nodes are in operation (*1)	Operating in both node or one side node (Online/No error)	Failover (*2) occurred due to a failure in the management port or in the cables.	Execute the flow of Figure C.2.3.2.2-2. 'C.2.3.2.2 Flow of Management Network Failure Determination (2) Failure in the management port or the cables'
						Stopping resource groups in both nodes (The status is srmd executable error) (*5)	The resource of the both nodes are stopped abnormally because a failure occurs on the maintenance port or the cable, and then restarting is occurred on the other side node.	
					Only one node is in operation (*1)	Operating in one side node (Online/No error)	Reset has been issued due to OS down, and then the failover (*2) has occurred.	'C.2.3.4 Determining the node failure when failover occurred'
4	Y	N	Y	N	—	—	Double or more failures in the ports or the cables have occurred.	'Table C.2.3.2.1-2 Failure Status (Determination of Multiple Failures of #4 through #6)'
5	Y	N	N	Y	—	—	Double or more failures in the ports or the cables occurred.	
6	N	N	Y	Y	—	—	A wrong setting of the management port IP address, both nodes' operating systems down, double or more failures in the ports and the cables, or a failure on the disk array subsystem occurred.	
7	N	N	N	N	Both nodes are in operation (*3)	Operating in both nodes (Online/No error)	A failure in the management IP-SW occurred.	Execute the flow of Figure C.2.3.2.2-10. 'C.2.3.2.2 Flow of Management Network Failure Determination (10) Failure in the management IP-SW'

Y: ping response is returned, N: ping response is not returned

Copyright © 2011, 2014, Hitachi, Ltd.

*1: At the site where the Management LAN IP-SW provided by (HDS) is installed, connect the maintenance PC to the management LAN IP-SW, and check the OS operation status by the ping confirmation for the node that cannot communicate with the management port. If the ping communication is available, determine that the both nodes are in operation.
At the site where the Management LAN IP-SW owned by the customer is installed, connect the maintenance PCs to the maintenance ports of the both nodes directly, and check the OS operation status by the ping confirmation. If the ping communication is available, determine that the both nodes are in operation.
If the ping communication is not available, just one side node is in operation.

*2: When the failover of resource group is complete, "Running node" of the both resource groups becomes the same node name. For the details about "Running node", refer to "Maintenance Tool '2.2 Displaying the Cluster Status (clstatus)' (MNTT 02-0040)".

*3: Connect the maintenance PC directly to the maintenance ports of both nodes and check the OS operation status by the ping communication. If the ping communication is available, determine that the node is in operation.

*4: Check the resource group operation status when the resource group is in operation. When both are in operation, check the both operation status.

Copyright © 2011, 2013, Hitachi, Ltd.

Table C.2.3.2.1-2 Failure Status (Determination of Multiple Failures of #4 through #6) (1/2)

Item number in Table C.2.3.2.1-1	Condition for determination		Details of failure	Recovery operation	Failure determination procedure (*3)
	Failover completion (*1)	OS operation status			
4	Y or N	Both nodes are in operation (*4)	Failures have occurred in the management port/cable, BMC port/cable of the same nodes.	Perform failover when the virtual IP address is set on the management port. The OS service continues running. Replace the failed part.	Execute the flow of Figure C.2.3.2.2-3.
	Y	Only one node is in operation (*4)	Failures of OS down and of BMC port/cable have occurred on the same node.	The OS service is continued. However terminate the service on the failure side, and then replace the failed part.	Execute the flow of Figure C.2.3.2.2-4.
5	Y or N	Both nodes are in operation (*2)	① A failure has occurred in the BMC port/cable. ② A failure has occurred also in the management port/cable of the other node.	Perform the management port recovery operation first, because if you perform the BMC port recovery operation first, the node in normal service must be terminated.	Execute the flow of Figure C.2.3.2.2-5.
	Y	Only one node is in operation (*2)	① Reset has been issued due to OS down, and the failover is being executed. ② A failure has occurred in the BMC port/cable of the other node.	Perform the replacement operation for the OS downed node first, because if you perform the replacement operation for the BMC port first, the node which can be failed over will not exist.	Execute the flow of Figure C.2.3.2.2-6.

*1: Failover completed: Y, Failover not completed: N.
When resource groups are in operation and the failovers are complete, "Running node" of the both resource groups becomes the same node name. For the details about "Running node", refer to "Maintenance Tool '2.2 Displaying the Cluster Status (clstatus)' (MNTT 02-0040)".

*2: Check the logon prompt indication for the node that cannot communicate with the management port with the connection by the remote console. In the node displaying the logon prompt, the OS is in operation. And for the node that can communicate with the management port, determine that the node is in operation.
For the remote console connection, refer to 'B.1.3 Connection Confirmation of the Remote Console' and for the OS operation status, refer to 'B.1.4 Startup Confirmation of the OS by Using Remote Console'.

*3: For the failure determination procedures, follow 'C.2.3.2.2 Flow of management network failure determination'.

*4: At the site where the Management LAN IP-SW provided by (HDS) is installed, connect the maintenance PC to the management LAN IP-SW, and check the OS operation status by the ping confirmation for the node that cannot communicate with the management port. If the ping communication is available, determine that the both nodes are in operation.
At the site where the Management LAN IP-SW owned by the customer is installed, connect the maintenance PCs to the maintenance ports of the both nodes directly, and check the OS operation status by the ping confirmation. If the ping communication is available, determine that the both nodes are in operation.
If the ping communication is not available, just one side node is in operation. In this case, borrow a monitor and a keyboard to be connected to the node from the system administrator because the confirmation might not be available by the remote console connection.

Copyright © 2011, 2013, Hitachi, Ltd.

Table C.2.3.2.1-2 Failure Status (Determination of Multiple Failures of #4 through #6) (2/2)

Item number in Table C.2.3.2.1-1	Condition for determination			Details of failure	Recovery operation	Failure determination procedure (*3)
	Failover completion (*1)	OS operation status (*2)	Resource group operation status (*5)			
6	Y or N	Both nodes are in operation	Both nodes are in operation (Online/No error)	Failures have occurred in the management port/cable of the both nodes. (*4)	As the communication is enabled via the heartbeat cable, the OS service is continued. Execute the replacement operation for each node one by one by terminating it by manual failover.	Execute the flow of Figure C.2.3.2.2-7.
	Y	Only one node is in operation	Only one node is in operation (Online/No error)	① Reset has been issued due to the OS outage, and the failover is being executed. ② After the failover completion, a failure has occurred in the management port/cable of the other node.	As the OS service is continued by the failover, execute the replacement operation by terminating the node of failed OS.	Execute the flow of Figure C.2.3.2.2-8.
	Y	Only one node is in operation	Resource groups of both nodes terminated (Error status is srmd executable error)	After a failure occurred on the side of the maintenance port and failover is executed, a failure of the service termination on both nodes occurred due to OS down on the other side node.	Terminate the node that failed, and recover it.	
	N	No node is in operation	Command cannot be executed because no node is in operation.	OS double failures have occurred.	Execute checking by using the diagnostic tool of the hardware vendor. Check also the Disk Array Subsystem.	Execute the flow of Figure C.2.3.2.2-9.

*1: Failover completed: Y, Failover not completed: N.
When the resource groups are in operation and the failovers are complete, "Running node" of the both resource groups becomes the same node name. For the details about "Running node", refer to "Maintenance Tool '2.2 Displaying the Cluster Status (clstatus)' (MNTT 02-0040)".

*2: Check the logon prompt indication of node by connecting the remote console. In the node displaying the logon prompt, the OS is in operation. By switching the logon prompt indication confirmation in each place of connecting node, the state of both nodes operation can be checked.
For the remote console connection, refer to 'B.1.3 Connection Confirmation of the Remote Console' and for the OS operation status, refer to 'B.1.4 Startup Confirmation of the OS by Using Remote Console'.

*3: For the failure determination procedures, follow 'C.2.3.2.2 Flow of management network failure determination'.

*4: There is a case that Failover does not occur, and a case that Failover has completed. Failover does not occur when a case that the maintenance ports of the both nodes have failed at the same time.

*5: Check the resource group operation status when the resource group is in operation. When both are in operation, check the both operation status.

Copyright © 2011, 2013, Hitachi, Ltd.

This page is for editorial purpose only.

Copyright © 2011, 2013, Hitachi, Ltd.

C.2.3.2.2 Flow of management network failure determination

By following this section, perform the operation of the management network failure determination based on the execution result of the ping command executed in C.2.3.2.1.

Execute the failure determination flow by following "Table C.2.3.2.1-1 Matrix of Management Network Failures" or "Table C.2.3.2.1-2 Failure Status (Determination of Multiple Failures of #4 through #6)".

(1) Failure in the BMC ports or the cables

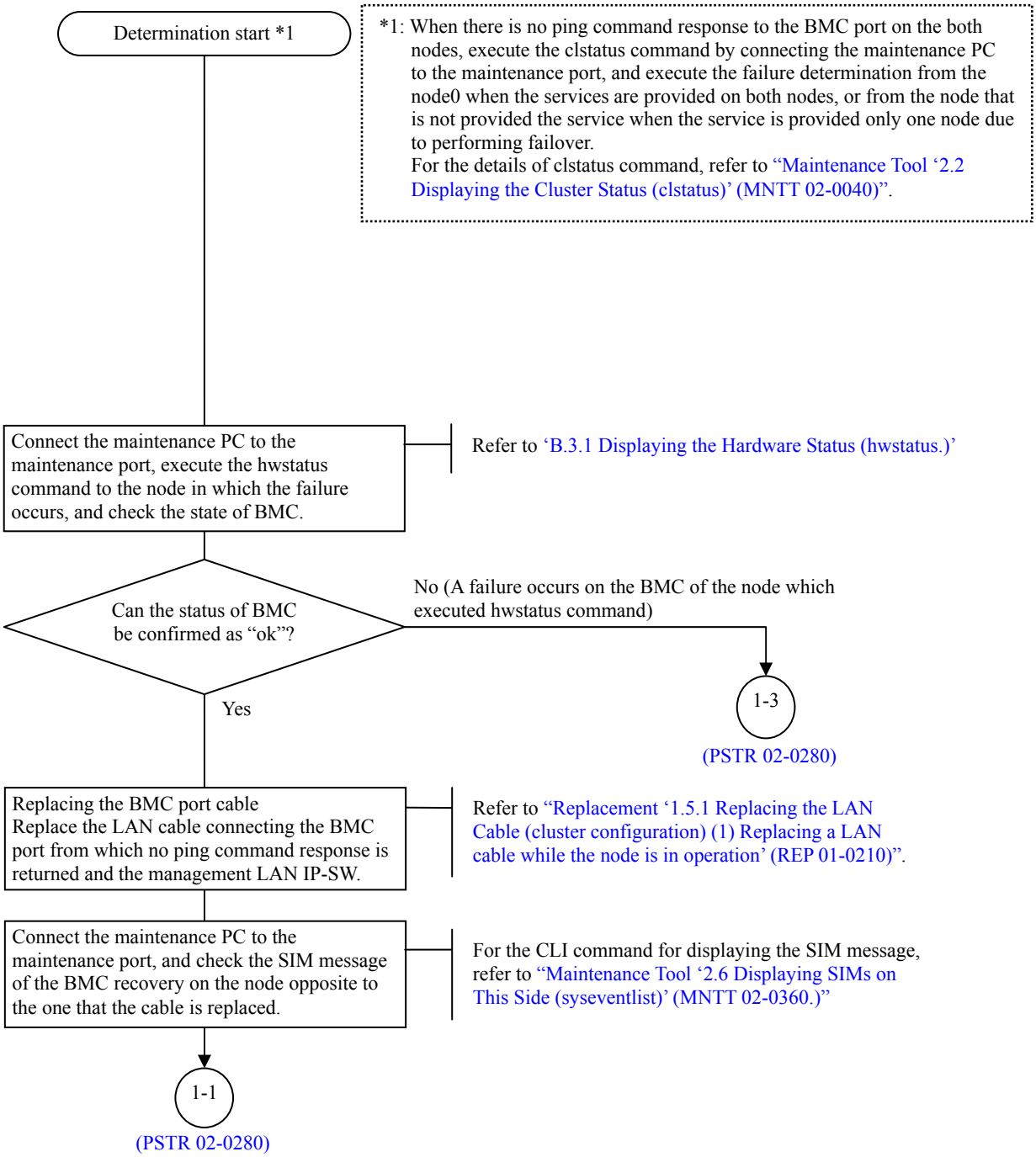


Figure C.2.3.2.2-1 Flow of Management Network Failure Determination (1/7)

Copyright © 2011, 2013, Hitachi, Ltd.

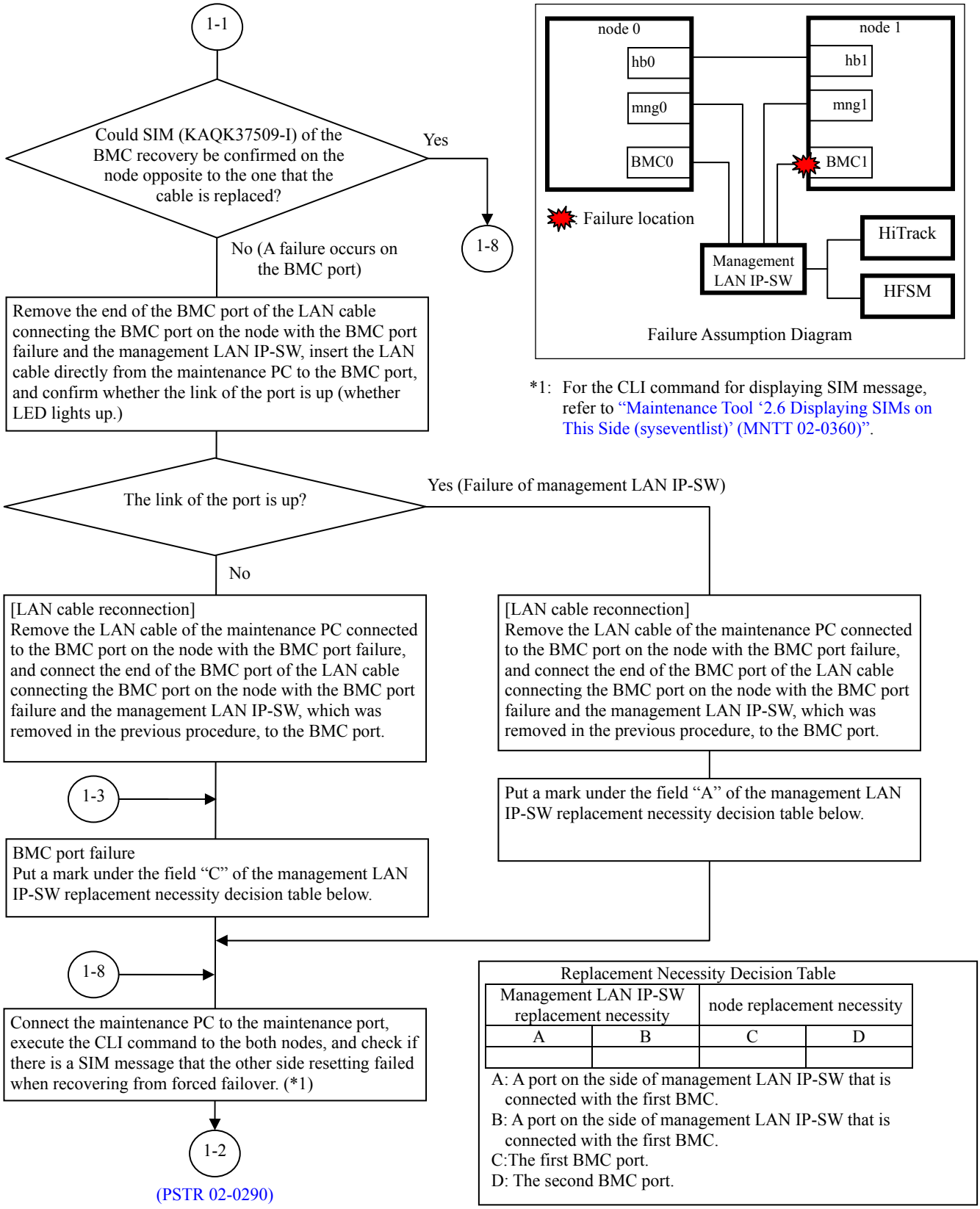
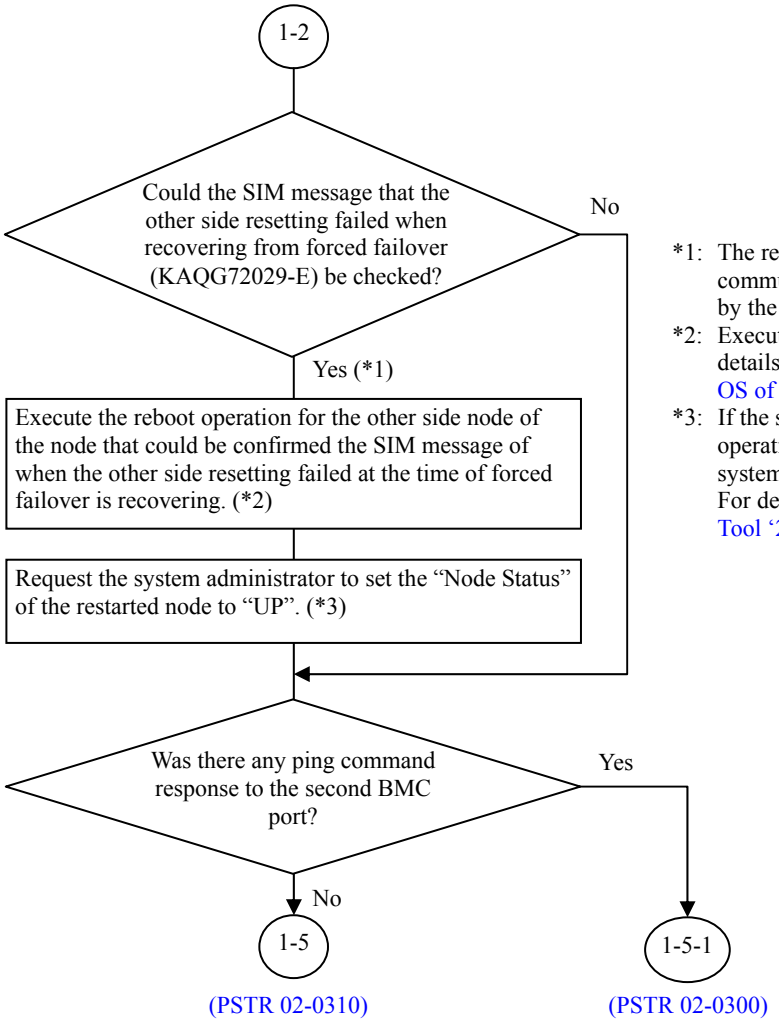


Figure C.2.3.2.2-1 Flow of Management Network Failure Determination (2/7)

Copyright © 2011, 2015, Hitachi, Ltd.



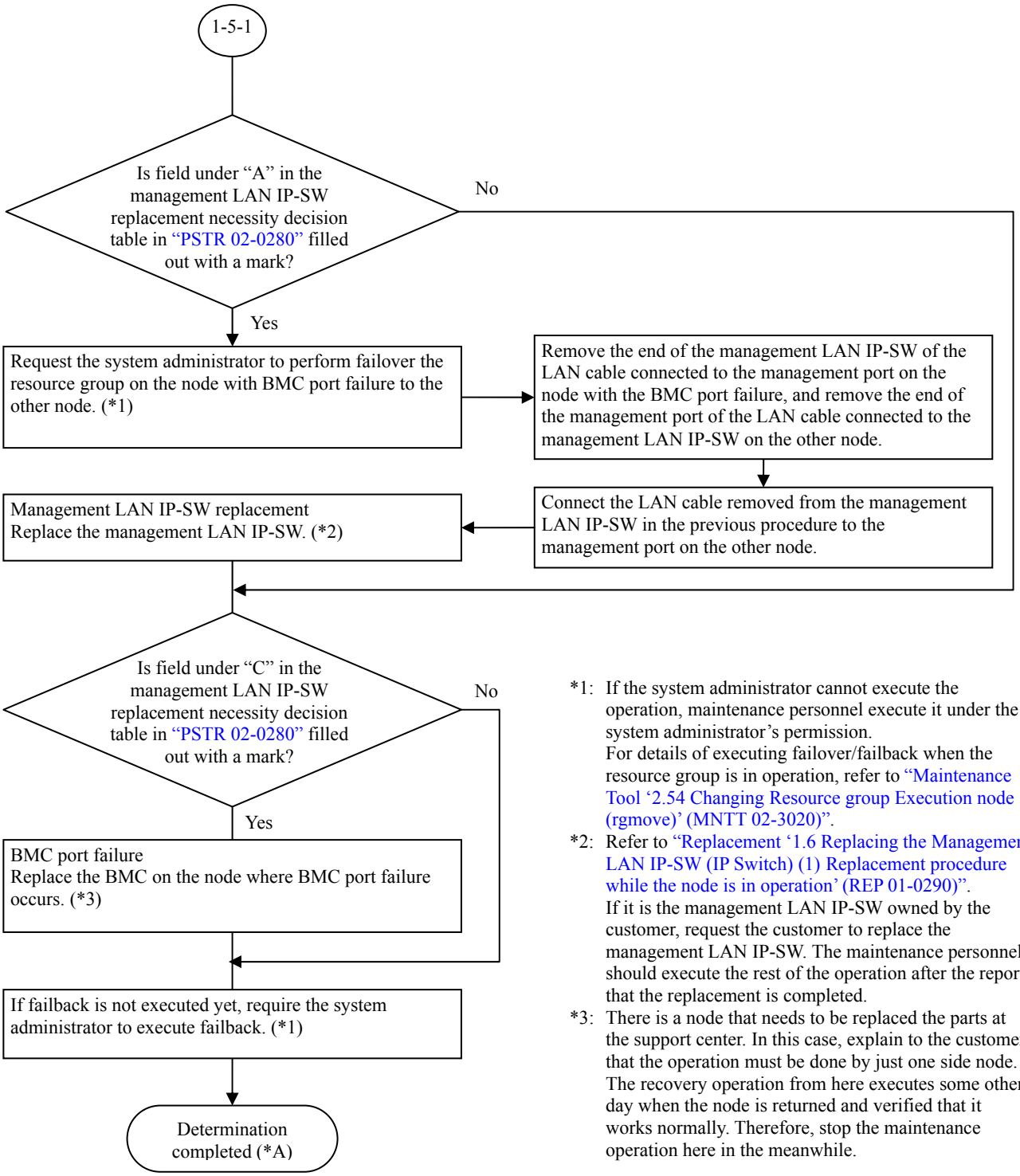
*1: The resetting at the time of recovering the heartbeat communication failed after the forced failover occurred by the restarting node on the side of failure BMC.

*2: Execute in the form of "nasreboot –force". For the details, refer to "Maintenance Tool '2.29 Rebooting the OS of This Side Node (nasreboot)' (MNTT 02-1790)".

*3: If the system administrator cannot execute the operation, maintenance personnel execute it under the system administrator's permission.
For details of starting a node, refer to "Maintenance Tool '2.50 Node Start Up (ndstart)' (MNTT 02-2760)".

Figure C.2.3.2.2-1 Flow of Management Network Failure Determination (3/7)

Copyright © 2011, 2013, Hitachi, Ltd.



*1: If the system administrator cannot execute the operation, maintenance personnel execute it under the system administrator's permission.
For details of executing failover/failback when the resource group is in operation, refer to "Maintenance Tool '2.54 Changing Resource group Execution node (rgmove)' (MNTT 02-3020)".

*2: Refer to "Replacement '1.6 Replacing the Management LAN IP-SW (IP Switch) (1) Replacement procedure while the node is in operation' (REP 01-0290)".
If it is the management LAN IP-SW owned by the customer, request the customer to replace the management LAN IP-SW. The maintenance personnel should execute the rest of the operation after the report that the replacement is completed.

*3: There is a node that needs to be replaced the parts at the support center. In this case, explain to the customer that the operation must be done by just one side node. The recovery operation from here executes some other day when the node is returned and verified that it works normally. Therefore, stop the maintenance operation here in the meanwhile.

*A: After completing determination, return to 'C.2.2.1 Failure determination procedure at the cluster configuration'.

Figure C.2.3.2.2-1 Flow of Management Network Failure Determination (4/7)

Copyright © 2011, 2013, Hitachi, Ltd.

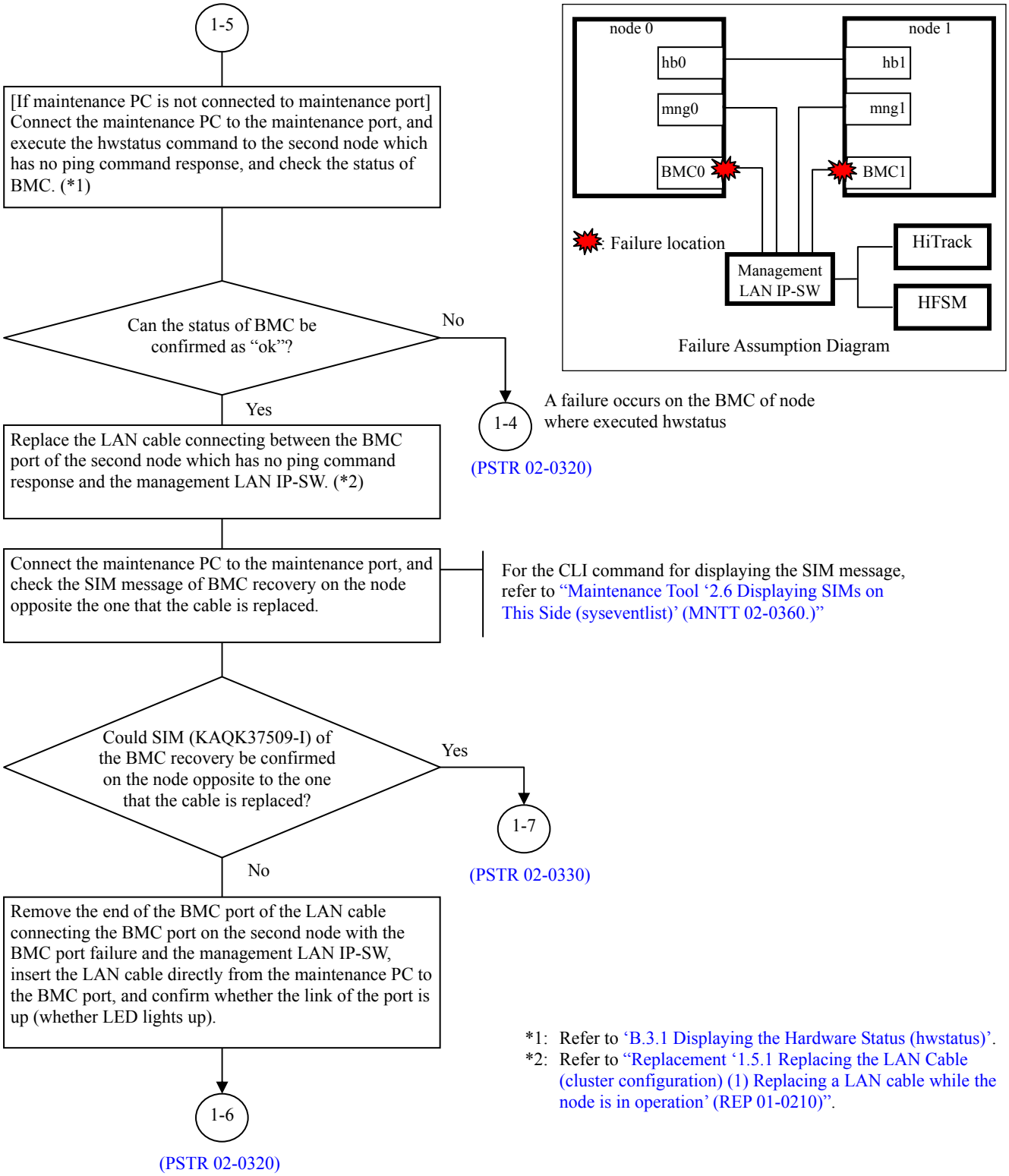
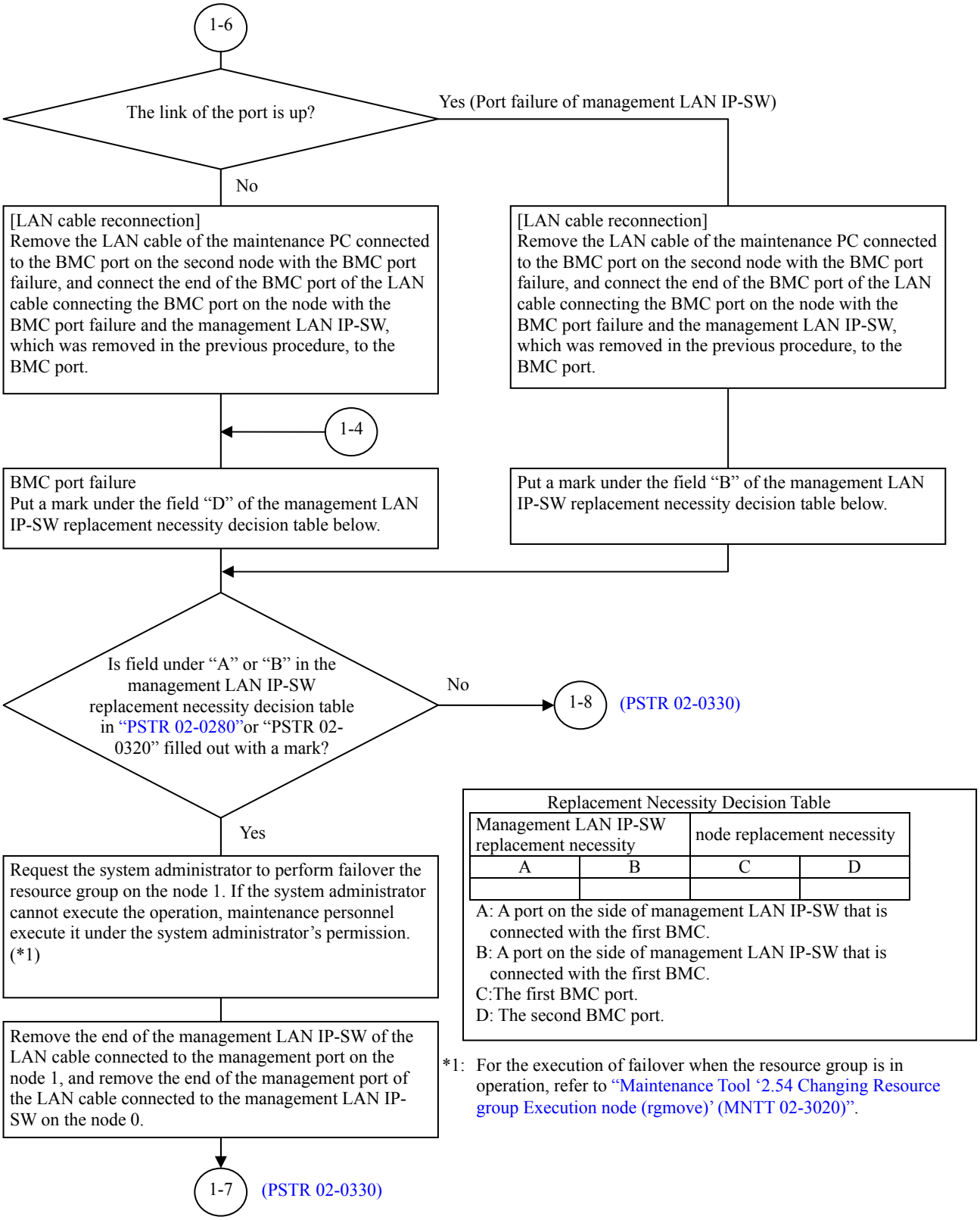


Figure C.2.3.2.2-1 Flow of Management Network Failure Determination (5/7)

Copyright © 2011, 2015, Hitachi, Ltd.



Replacement Necessity Decision Table

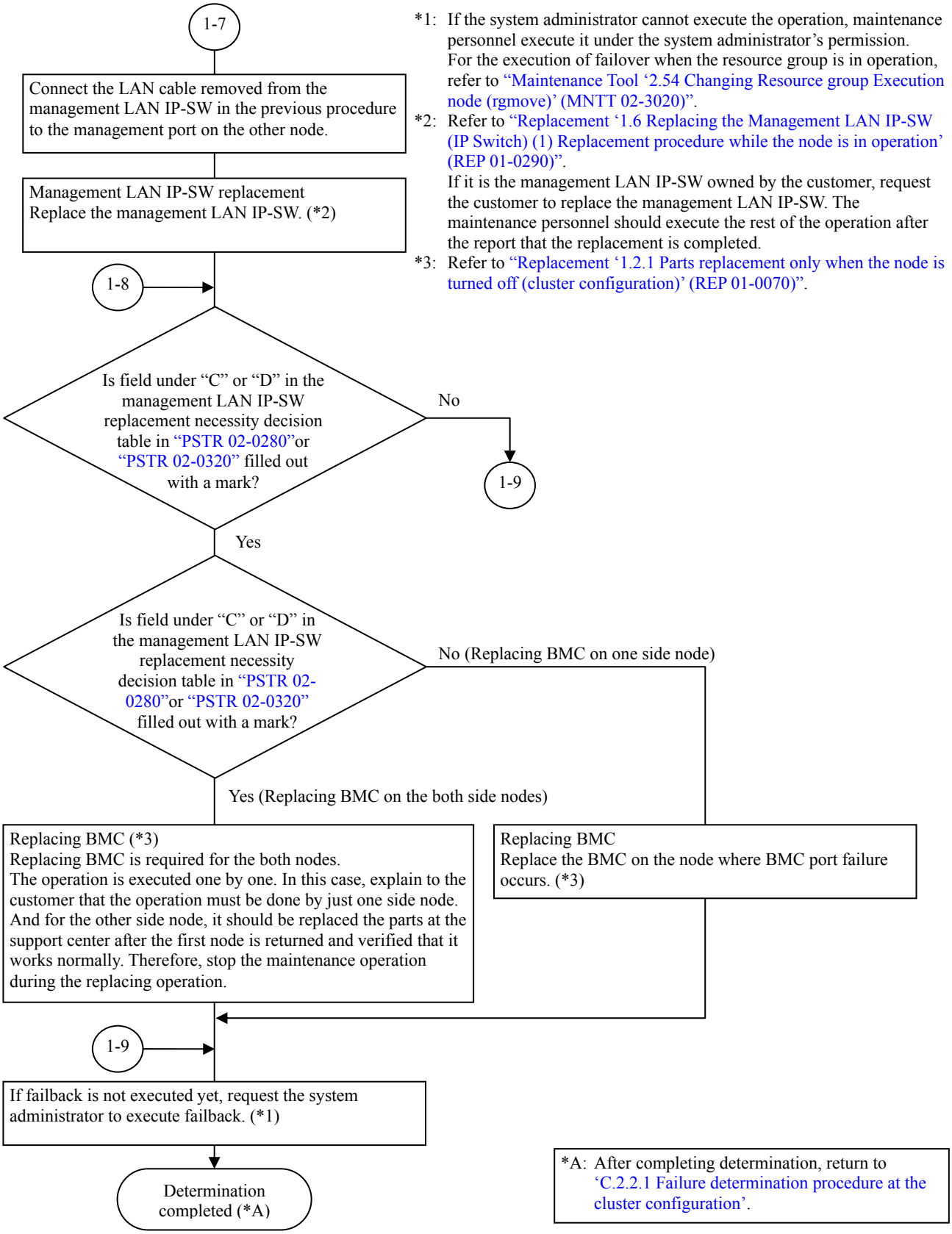
Management LAN IP-SW replacement necessity		node replacement necessity	
A	B	C	D

A: A port on the side of management LAN IP-SW that is connected with the first BMC.
B: A port on the side of management LAN IP-SW that is connected with the first BMC.
C:The first BMC port.
D: The second BMC port.

*1: For the execution of failover when the resource group is in operation, refer to "Maintenance Tool '2.54 Changing Resource group Execution node (rgmove)' (MNTT 02-3020)".

Figure C.2.3.2.2-1 Flow of Management Network Failure Determination (6/7)

Copyright © 2011, 2013, Hitachi, Ltd.



*1: If the system administrator cannot execute the operation, maintenance personnel execute it under the system administrator's permission. For the execution of failover when the resource group is in operation, refer to "Maintenance Tool '2.54 Changing Resource group Execution node (rgmove)' (MNTT 02-3020)".

*2: Refer to "Replacement '1.6 Replacing the Management LAN IP-SW (IP Switch) (1) Replacement procedure while the node is in operation' (REP 01-0290)". If it is the management LAN IP-SW owned by the customer, request the customer to replace the management LAN IP-SW. The maintenance personnel should execute the rest of the operation after the report that the replacement is completed.

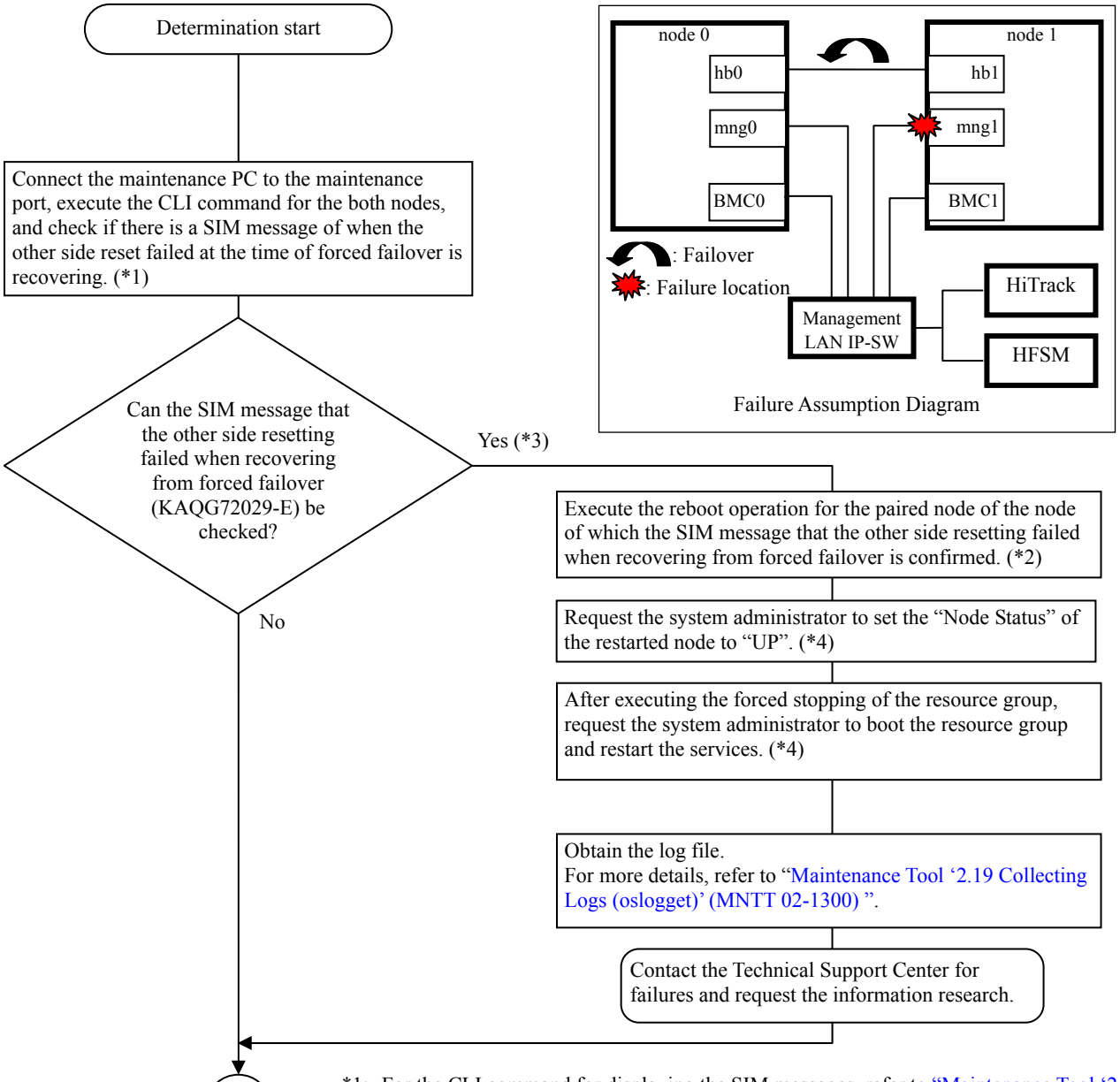
*3: Refer to "Replacement '1.2.1 Parts replacement only when the node is turned off (cluster configuration)' (REP 01-0070)".

*A: After completing determination, return to 'C.2.2.1 Failure determination procedure at the cluster configuration'.

Figure C.2.3.2.2-1 Flow of Management Network Failure Determination (7/7)

Copyright © 2011, 2014, Hitachi, Ltd.

(2) Failure in the management port or the cables



*1: For the CLI command for displaying the SIM messages, refer to "Maintenance Tool '2.6 Displaying SIMs on This Side (syseventlist)' (MNTT 02-0360)".

*2: Execute in the form of "nasreboot –force". For the details, refer to "Maintenance Tool '2.29 Rebooting the OS of This Side Node (nasreboot)' (MNTT 02-1790)".

*3: The resetting at the time of recovering the heartbeat communication failed, after the occurrence of a forced failover by rebooting of node that opposite to the one where a failure occurred on the maintenance port. [srmd executable error] is displayed on the error status of a resource group.

*4: If the system administrator cannot execute the operation, maintenance personnel execute it under the system administrator's permission. For details of starting a node, refer to "Maintenance Tool '2.50 Node Start Up (ndstart)' (MNTT 02-2760)".
For terminating a resource group, refer to "Maintenance Tool '3.3 The Operation Accompanying Forced Stop of the Resource group' (MNTT 03-0060)".

Figure C.2.3.2.2-2 Flow of Management Network Failure Determination (1/2)

Copyright © 2011, 2015, Hitachi, Ltd.

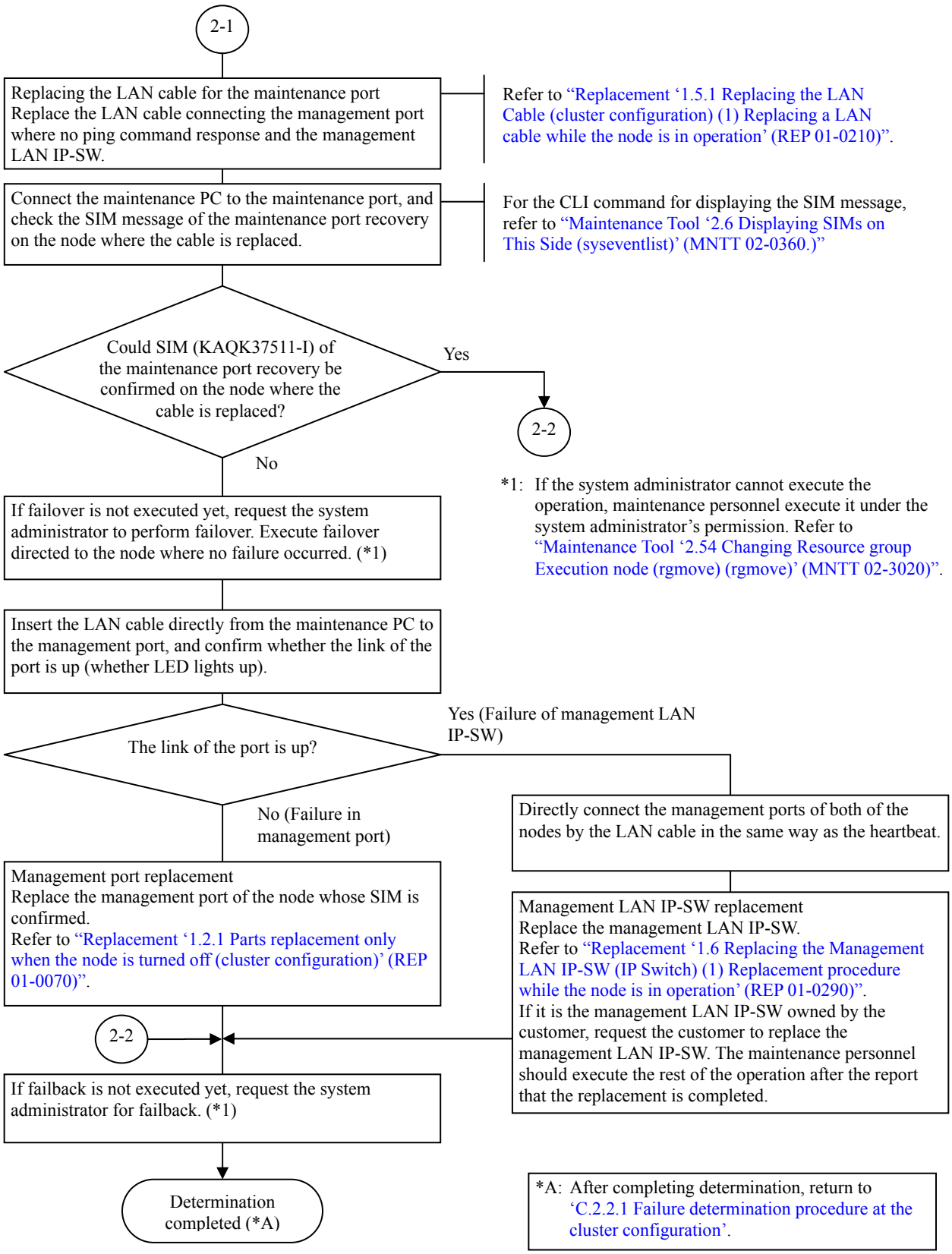


Figure C.2.3.2.2-2 Flow of Management Network Failure Determination (2/2)

Copyright © 2011, 2013, Hitachi, Ltd.

(3) Double failures in the port or cable

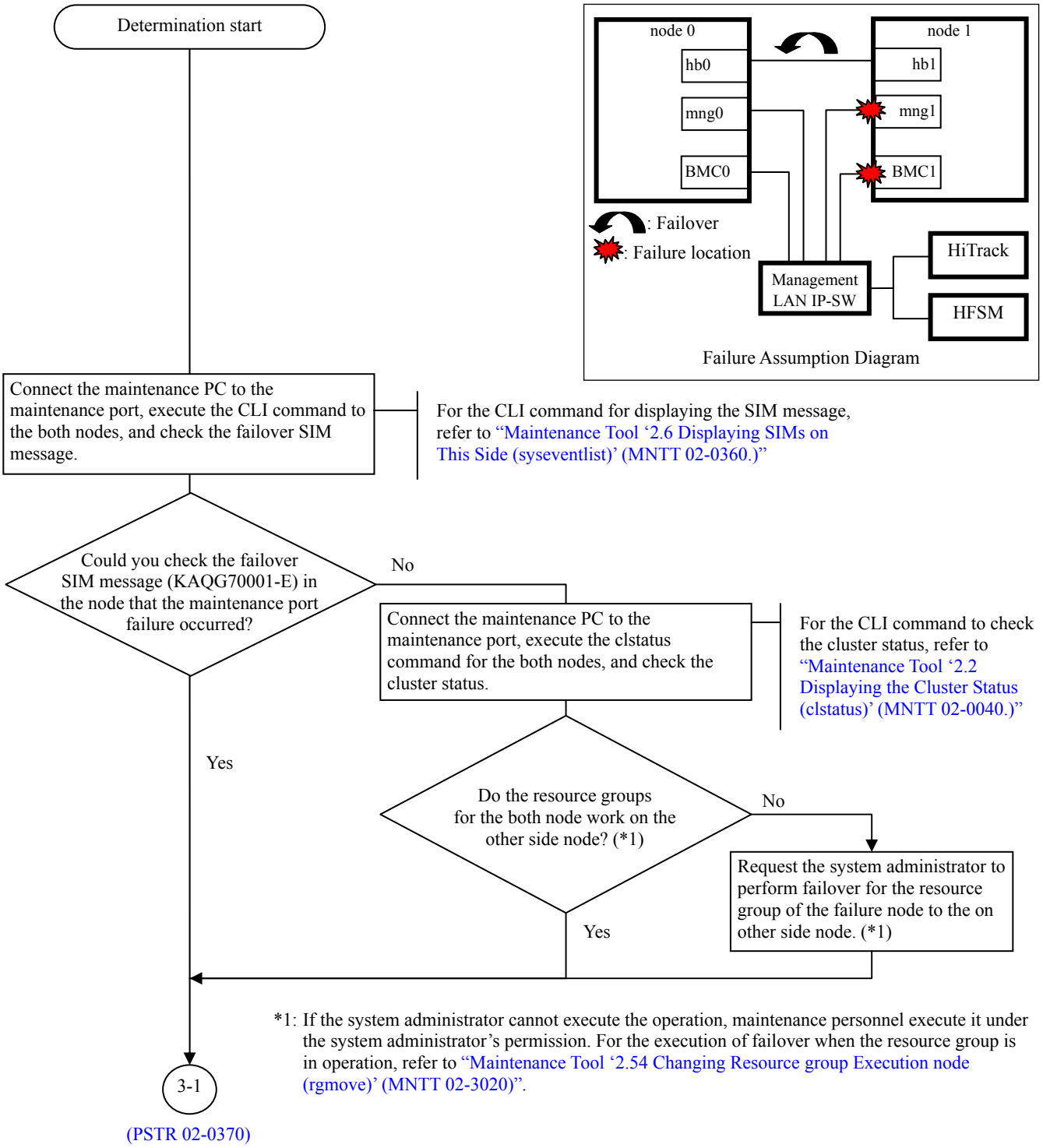


Figure C.2.3.2.2-3 Flow of Management Network Failure Determination (1/7)

Copyright © 2011, 2017, Hitachi, Ltd.

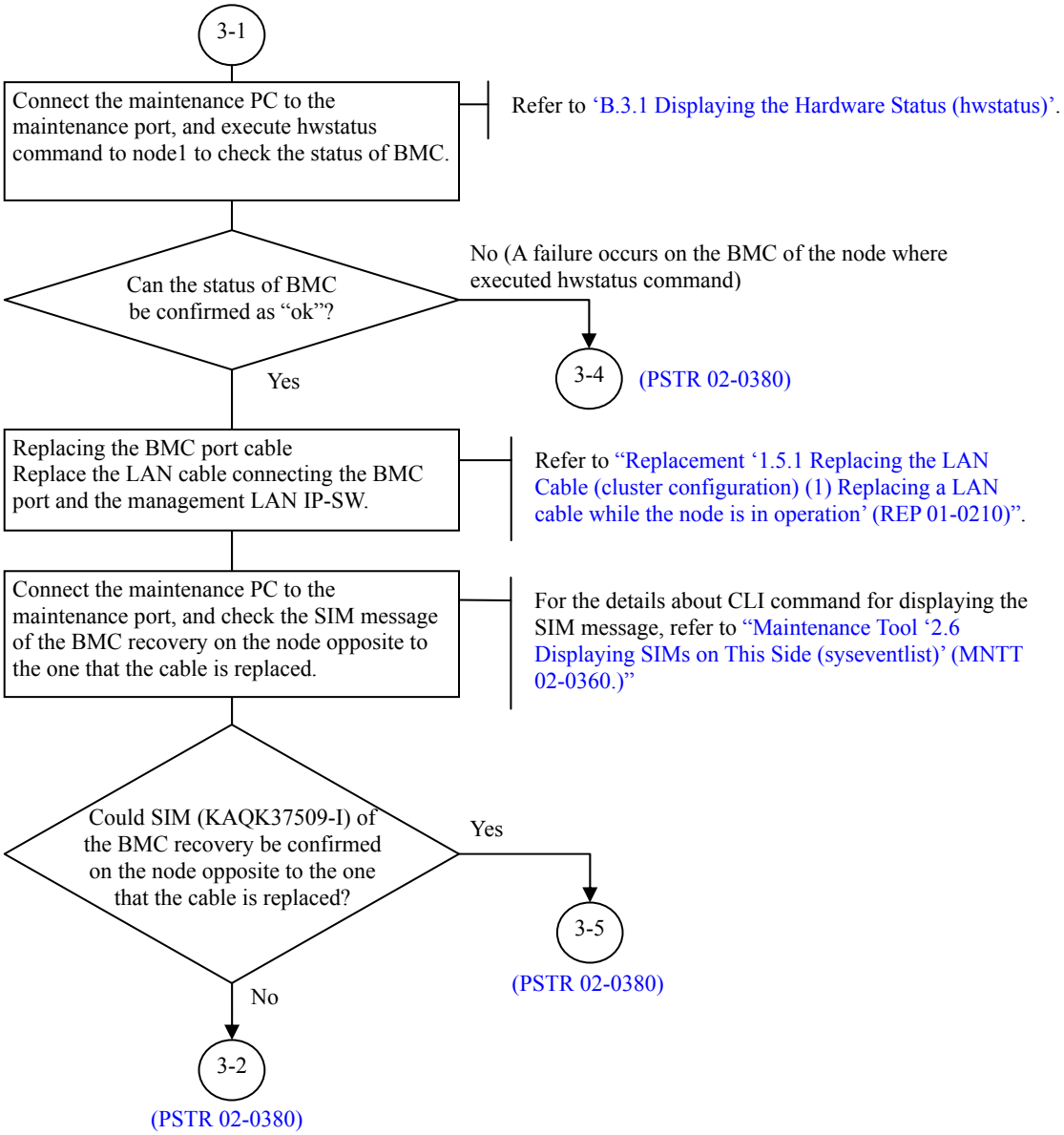
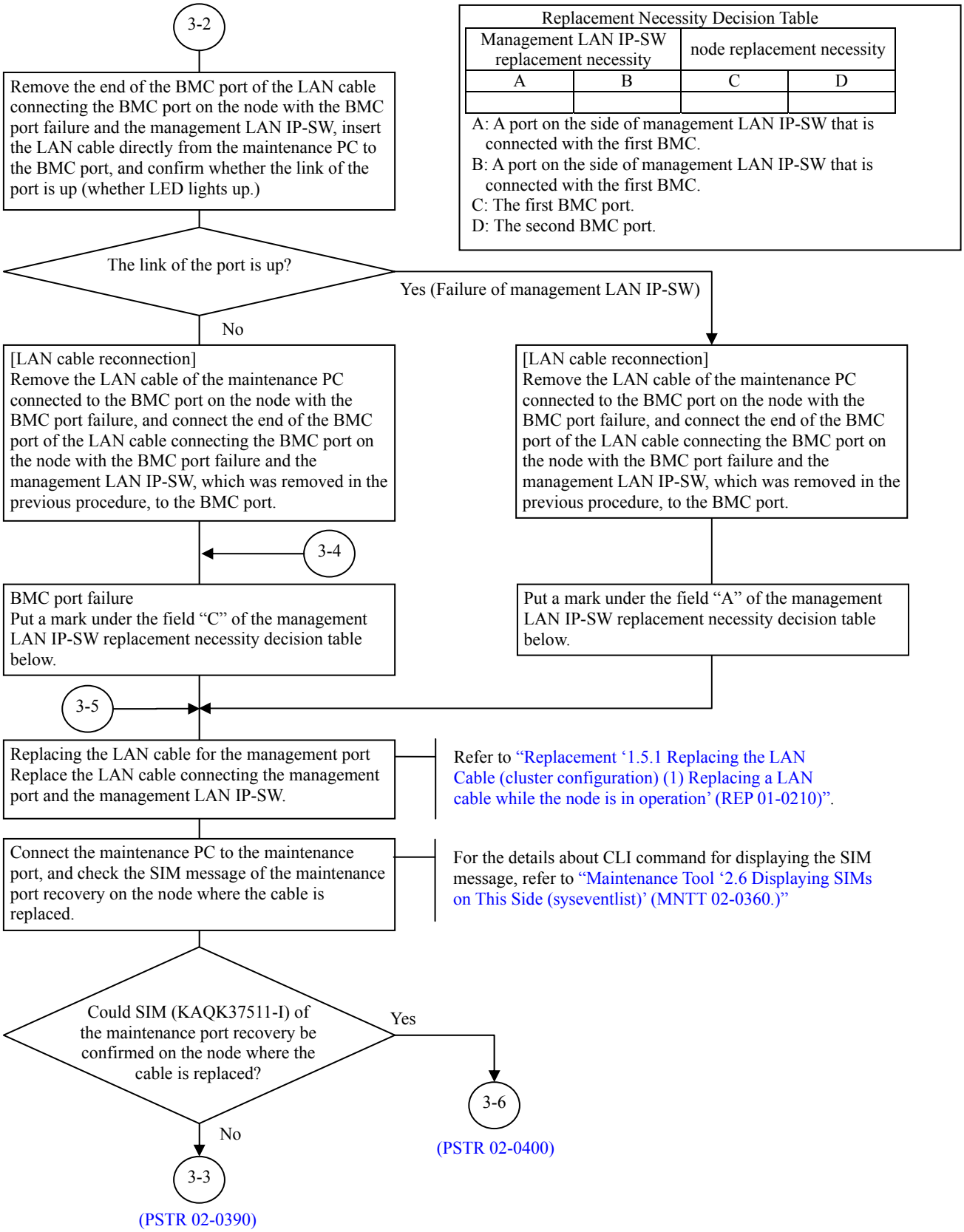


Figure C.2.3.2.2-3 Flow of Management Network Failure Determination (2/7)

Copyright © 2011, 2013, Hitachi, Ltd.



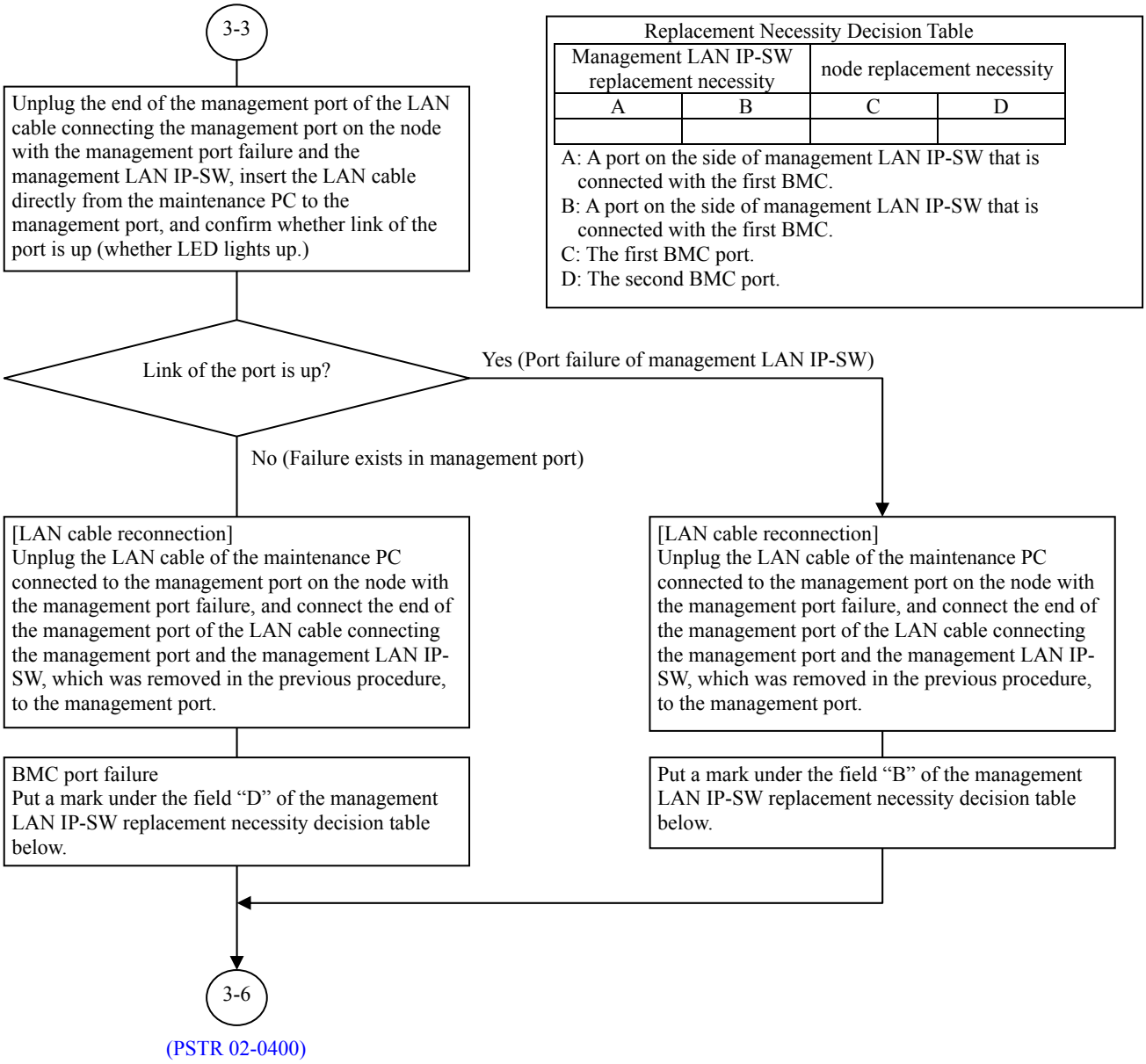
Replacement Necessity Decision Table

Management LAN IP-SW replacement necessity		node replacement necessity	
A	B	C	D

A: A port on the side of management LAN IP-SW that is connected with the first BMC.
B: A port on the side of management LAN IP-SW that is connected with the first BMC.
C: The first BMC port.
D: The second BMC port.

Figure C.2.3.2.2-3 Flow of Management Network Failure Determination (3/7)

Copyright © 2011, 2013, Hitachi, Ltd.



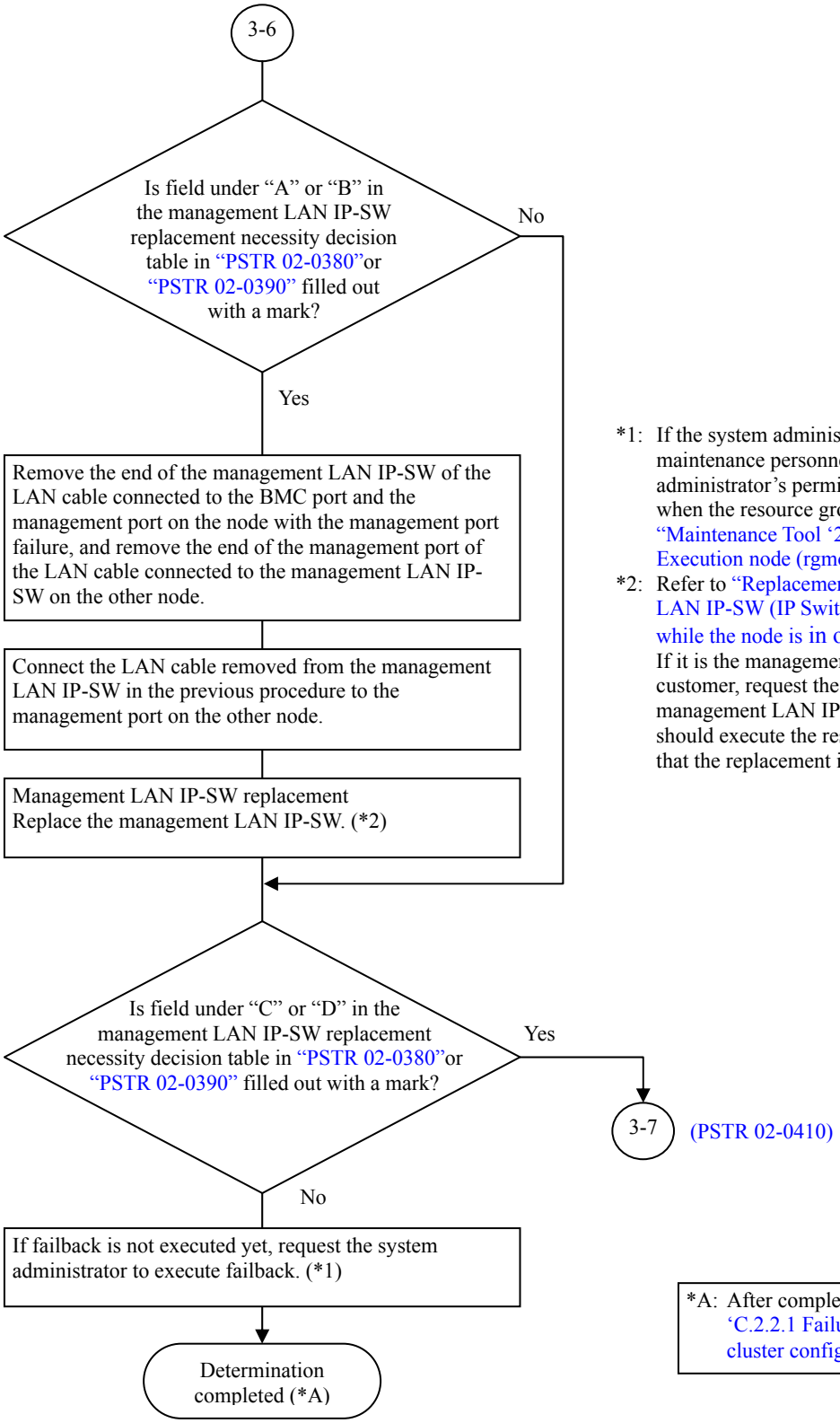
Replacement Necessity Decision Table

Management LAN IP-SW replacement necessity		node replacement necessity	
A	B	C	D

A: A port on the side of management LAN IP-SW that is connected with the first BMC.
B: A port on the side of management LAN IP-SW that is connected with the first BMC.
C: The first BMC port.
D: The second BMC port.

Figure C.2.3.2.2-3 Flow of Management Network Failure Determination (4/7)

Copyright © 2011, 2013, Hitachi, Ltd.



*1: If the system administrator cannot execute the operation, maintenance personnel execute it under the system administrator's permission. For the execution of failover when the resource group is in operation, refer to "Maintenance Tool '2.54 Changing Resource group Execution node (rgmove)' (MNTT 02-3020)".

*2: Refer to "Replacement '1.6 Replacing the Management LAN IP-SW (IP Switch) (1) Replacement procedure while the node is in operation' (REP 01-0290)".
If it is the management LAN IP-SW owned by the customer, request the customer to replace the management LAN IP-SW. The maintenance personnel should execute the rest of the operation after the report that the replacement is completed.

*A: After completing determination, return to 'C.2.2.1 Failure determination procedure at the cluster configuration'.

Figure C.2.3.2.2-3 Flow of Management Network Failure Determination (5/7)

Copyright © 2011, 2013, Hitachi, Ltd.

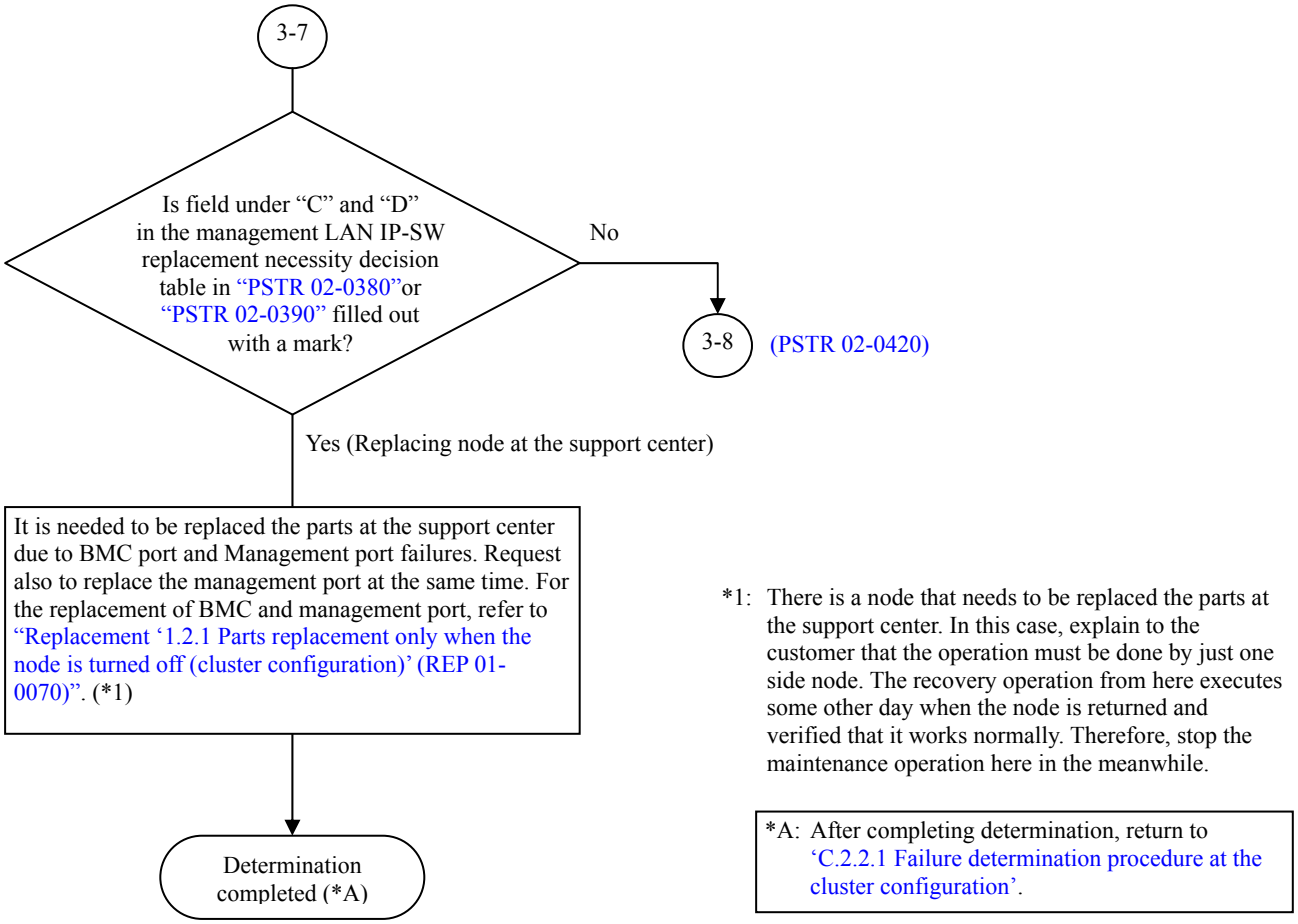
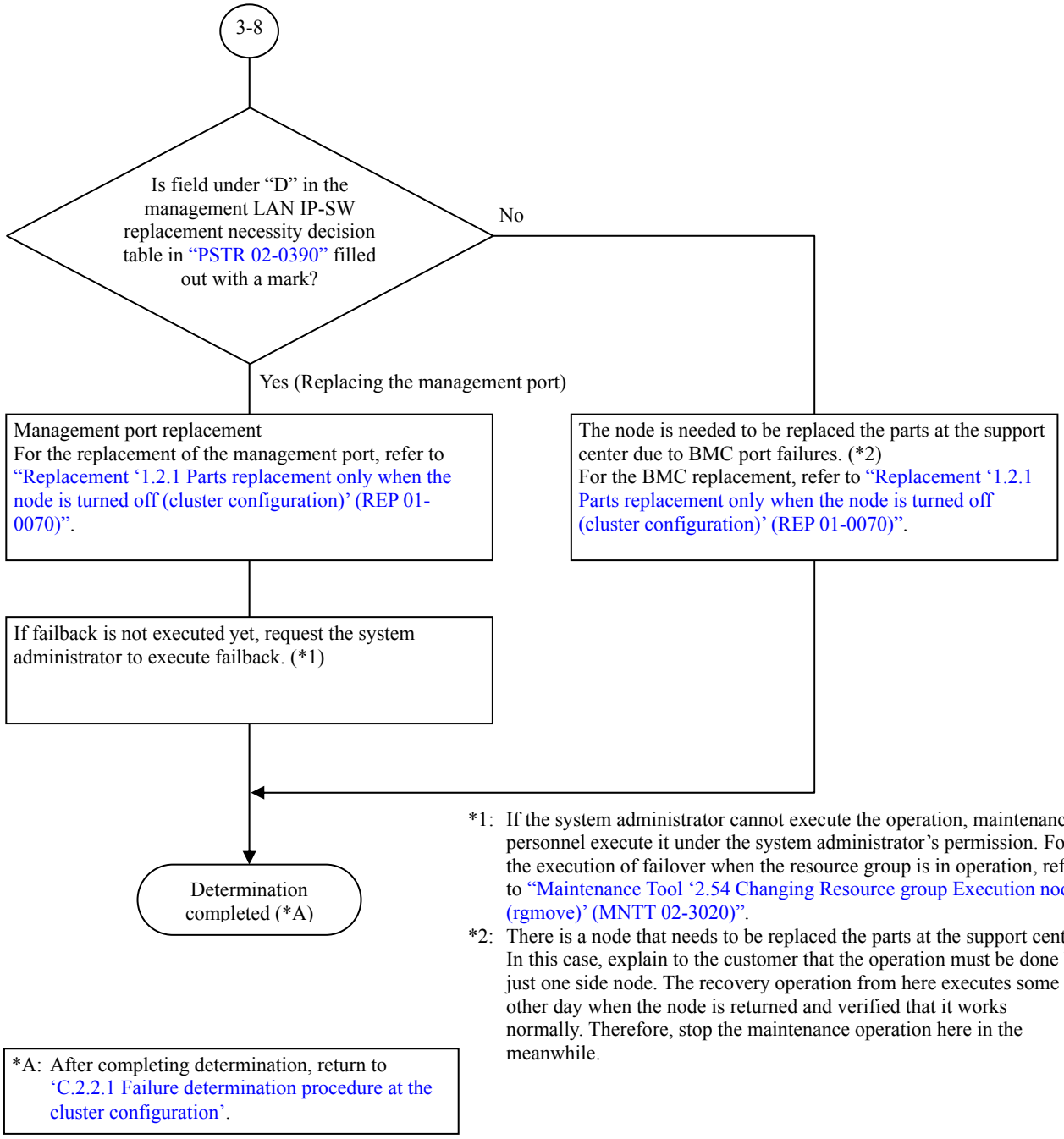


Figure C.2.3.2.2-3 Flow of Management Network Failure Determination (6/7)

Copyright © 2011, 2013, Hitachi, Ltd.



*1: If the system administrator cannot execute the operation, maintenance personnel execute it under the system administrator's permission. For the execution of failover when the resource group is in operation, refer to "Maintenance Tool '2.54 Changing Resource group Execution node (rgmove)' (MNTT 02-3020)".

*2: There is a node that needs to be replaced the parts at the support center. In this case, explain to the customer that the operation must be done by just one side node. The recovery operation from here executes some other day when the node is returned and verified that it works normally. Therefore, stop the maintenance operation here in the meanwhile.

Figure C.2.3.2.2-3 Flow of Management Network Failure Determination (7/7)

Copyright © 2011, 2013, Hitachi, Ltd.

(4) OS down and the failure in the BMC port on the same node

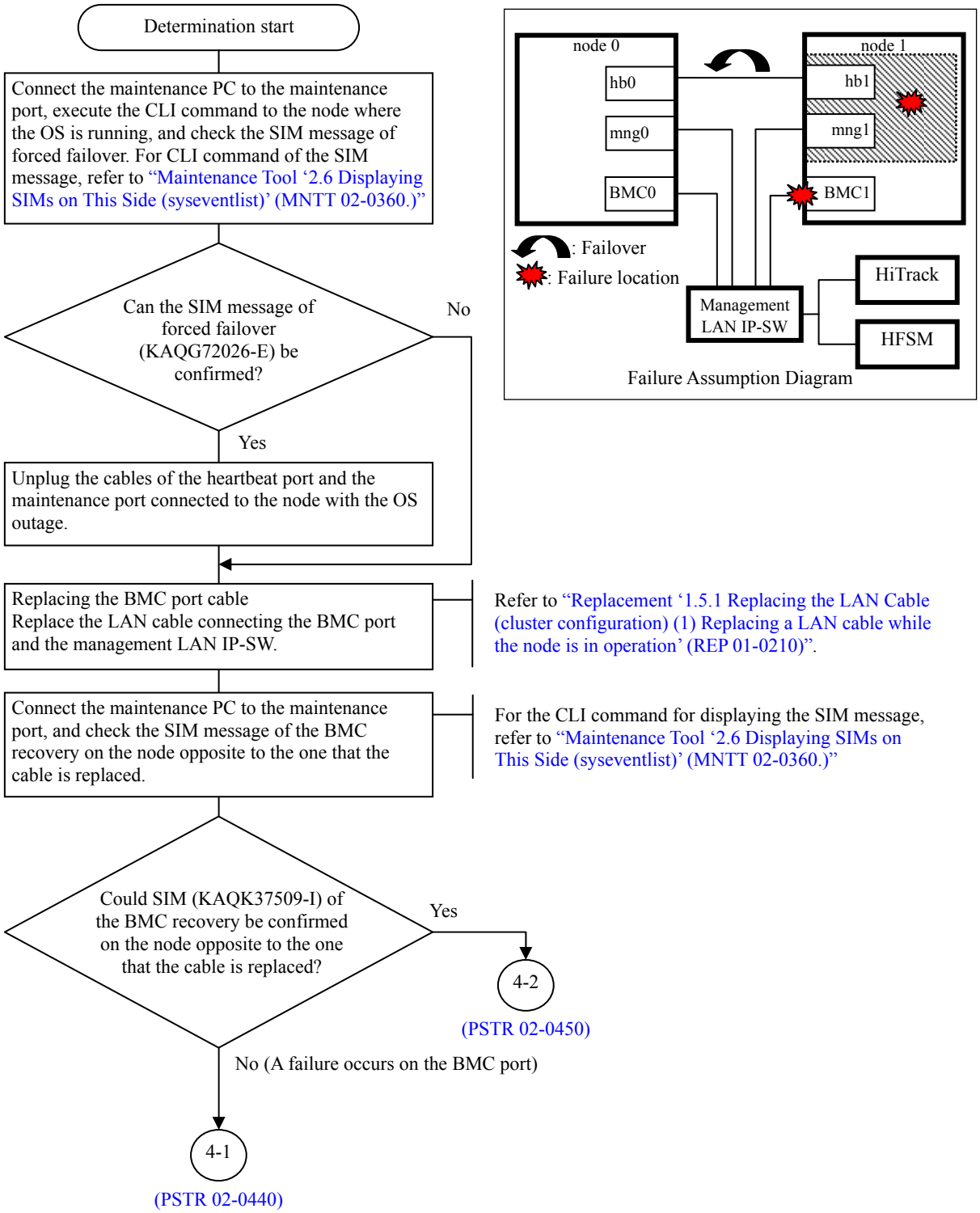


Figure C.2.3.2.2-4 Flow of Management Network Failure Determination (1/9)

Copyright © 2011, 2015, Hitachi, Ltd.

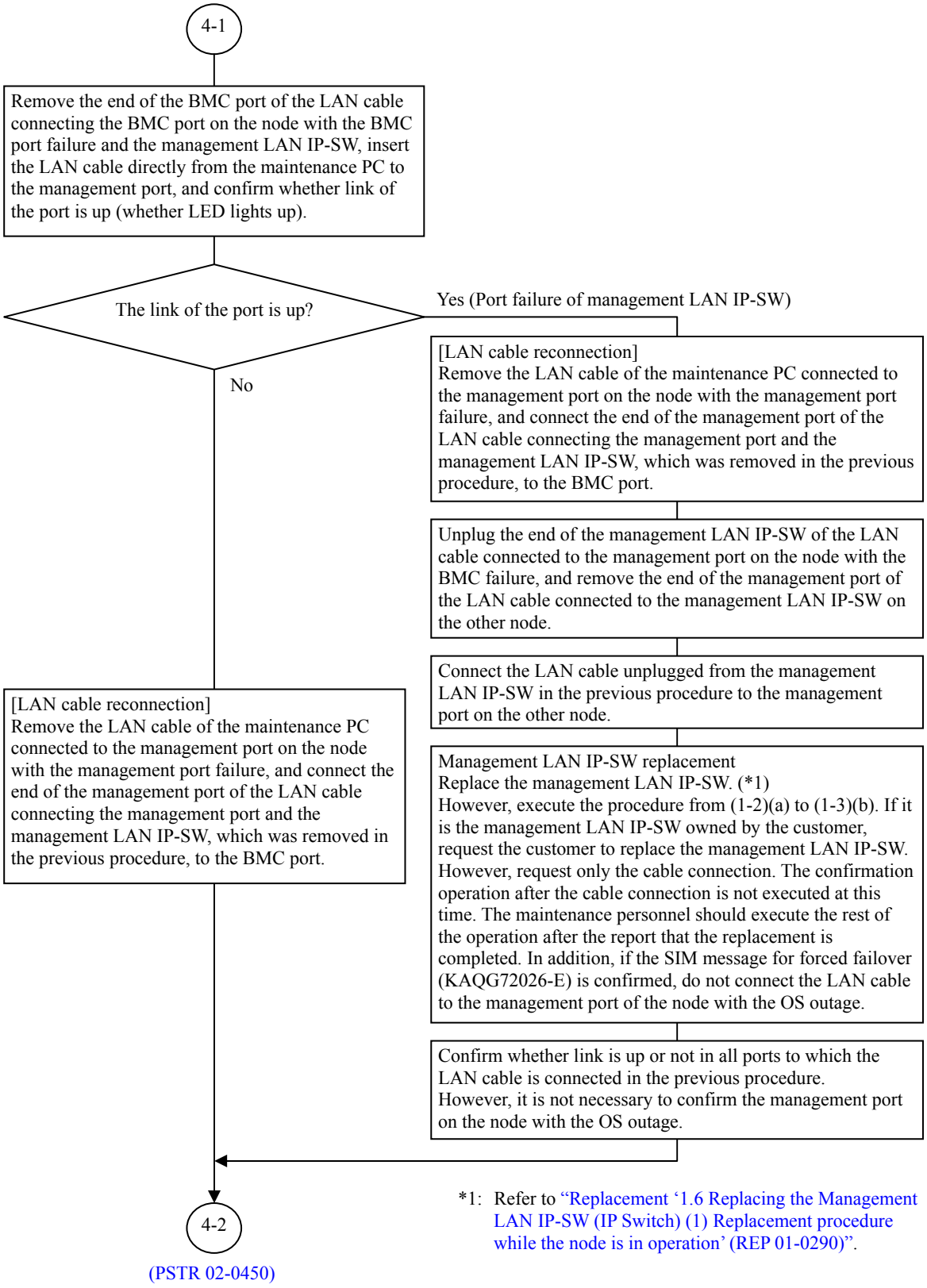
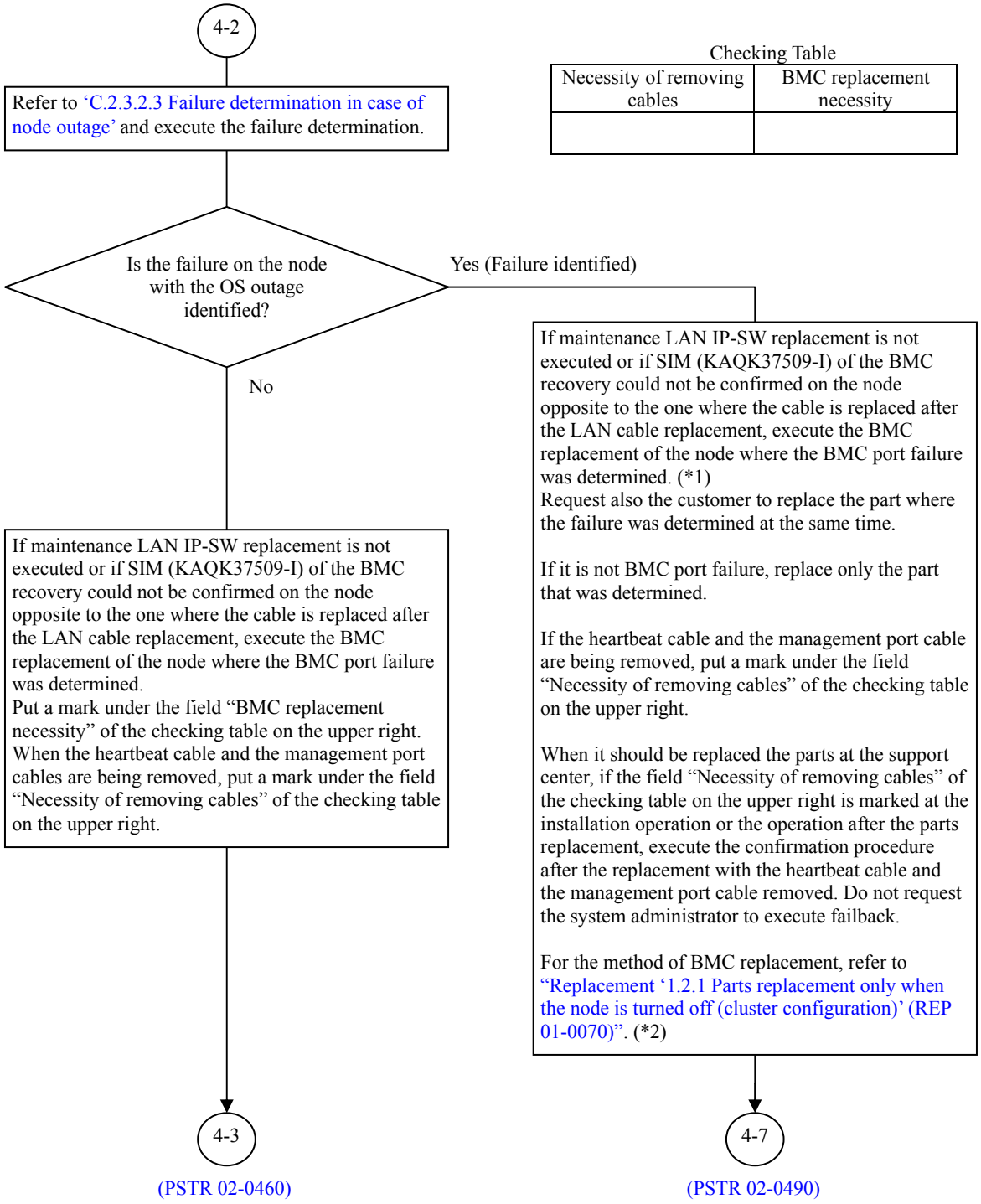


Figure C.2.3.2.2-4 Flow of Management Network Failure Determination (2/9)

Copyright © 2011, 2015, Hitachi, Ltd.

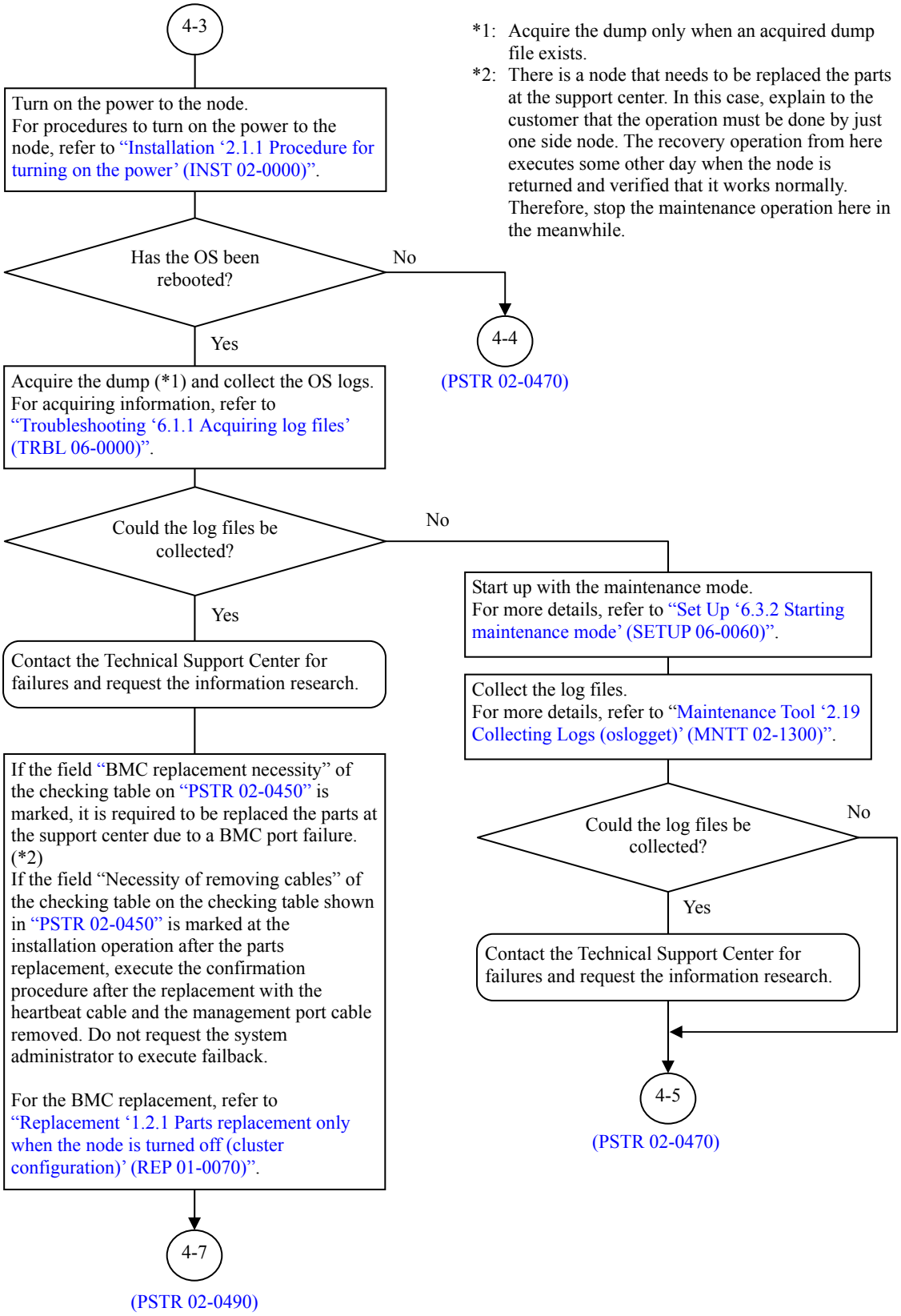


*1: There is a node that needs to be replaced the parts at the support center. In this case, explain to the customer that the operation must be done by just one side node. The recovery operation from here executes some other day when the node is returned and verified that it works normally. Therefore, stop the maintenance operation here in the meanwhile.

*2: Make sure to collect Simple log by using HATP before the parts replacement.

Figure C.2.3.2.2-4 Flow of Management Network Failure Determination (3/9)

Copyright © 2011, 2013, Hitachi, Ltd.



*1: Acquire the dump only when an acquired dump file exists.
*2: There is a node that needs to be replaced the parts at the support center. In this case, explain to the customer that the operation must be done by just one side node. The recovery operation from here executes some other day when the node is returned and verified that it works normally. Therefore, stop the maintenance operation here in the meanwhile.

Figure C.2.3.2.2-4 Flow of Management Network Failure Determination (4/9)

Copyright © 2011, 2015, Hitachi, Ltd.

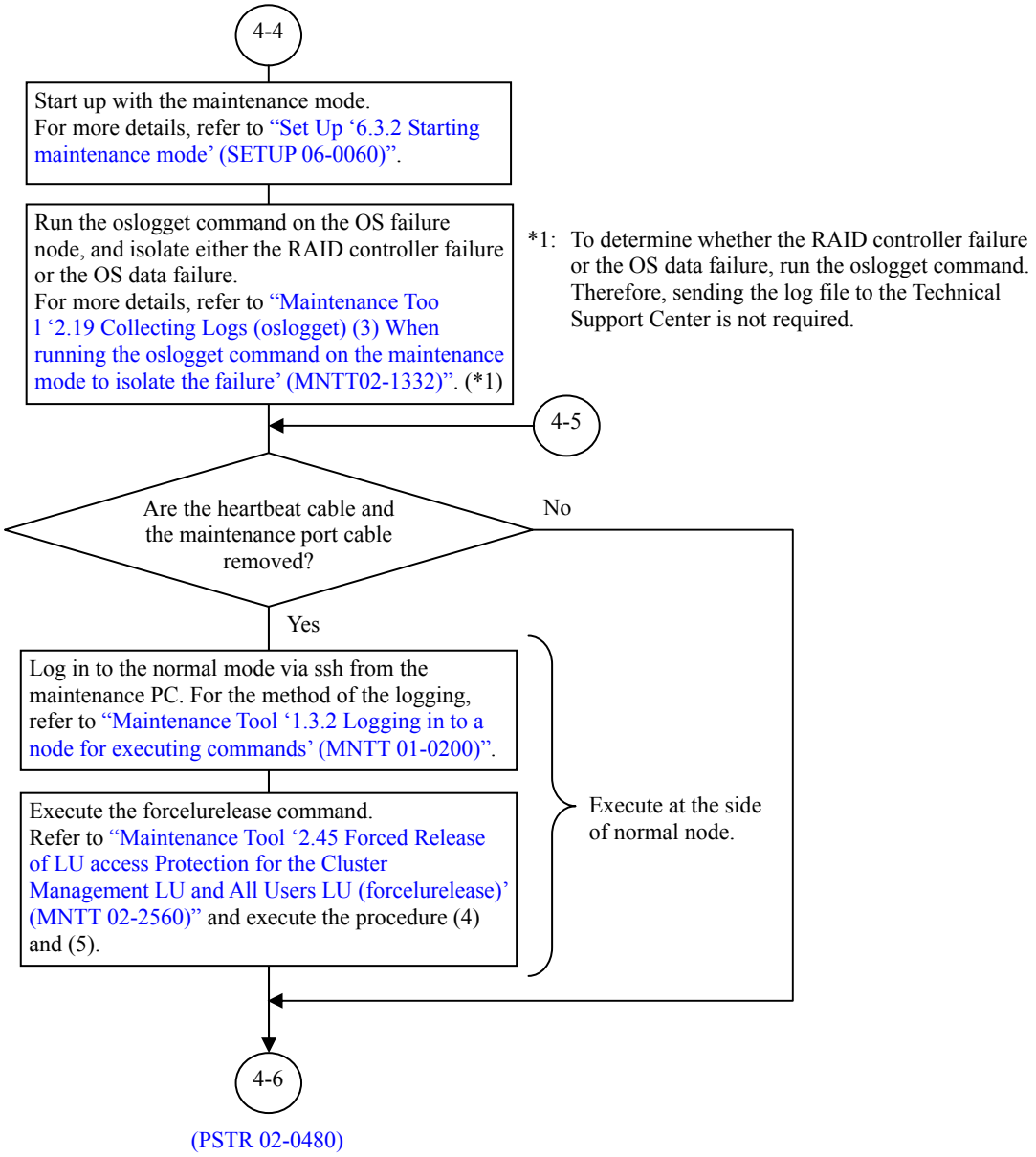
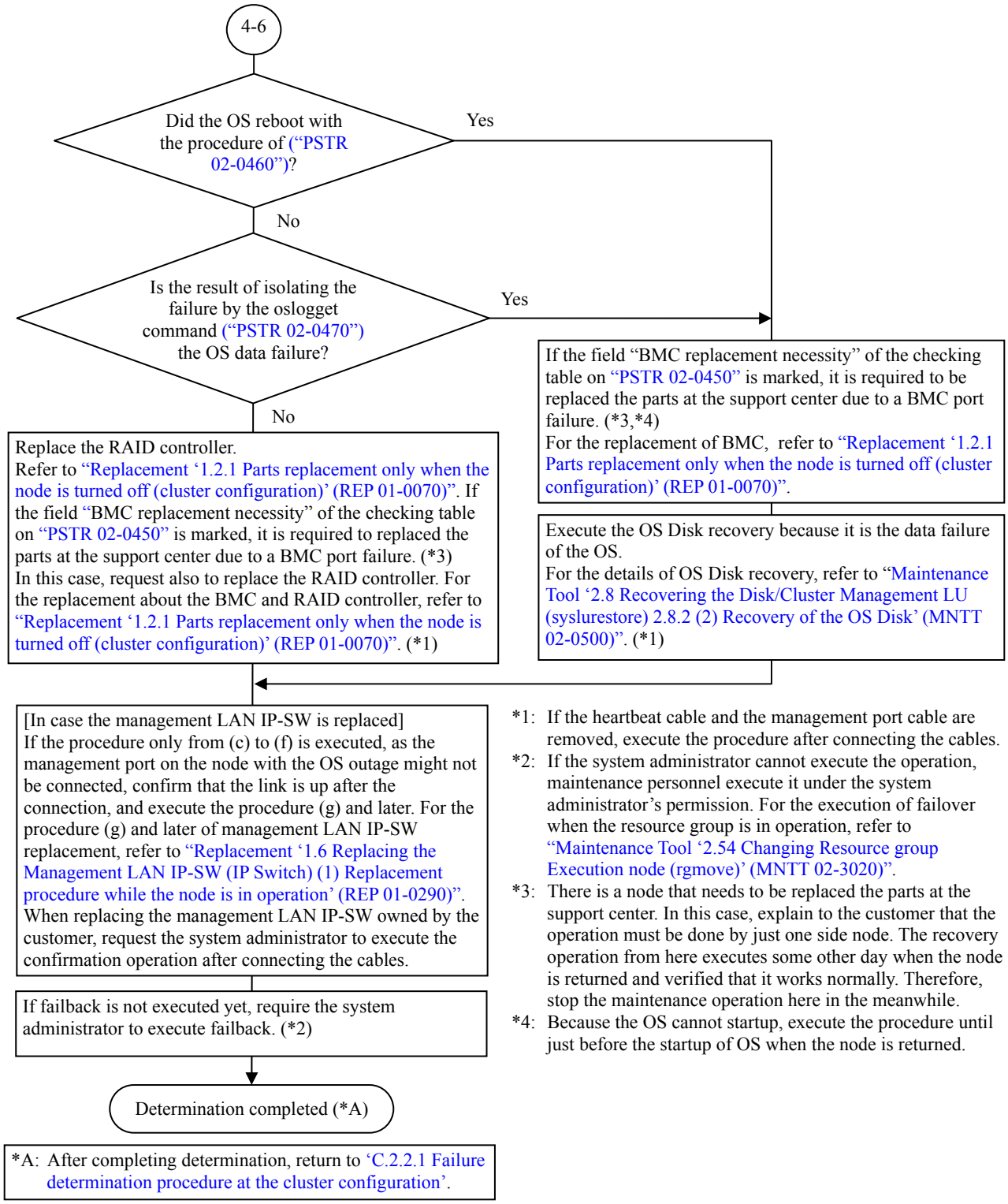


Figure C.2.3.2.2-4 Flow of Management Network Failure Determination (5/9)

Copyright © 2011, 2015, Hitachi, Ltd.



*1: If the heartbeat cable and the management port cable are removed, execute the procedure after connecting the cables.

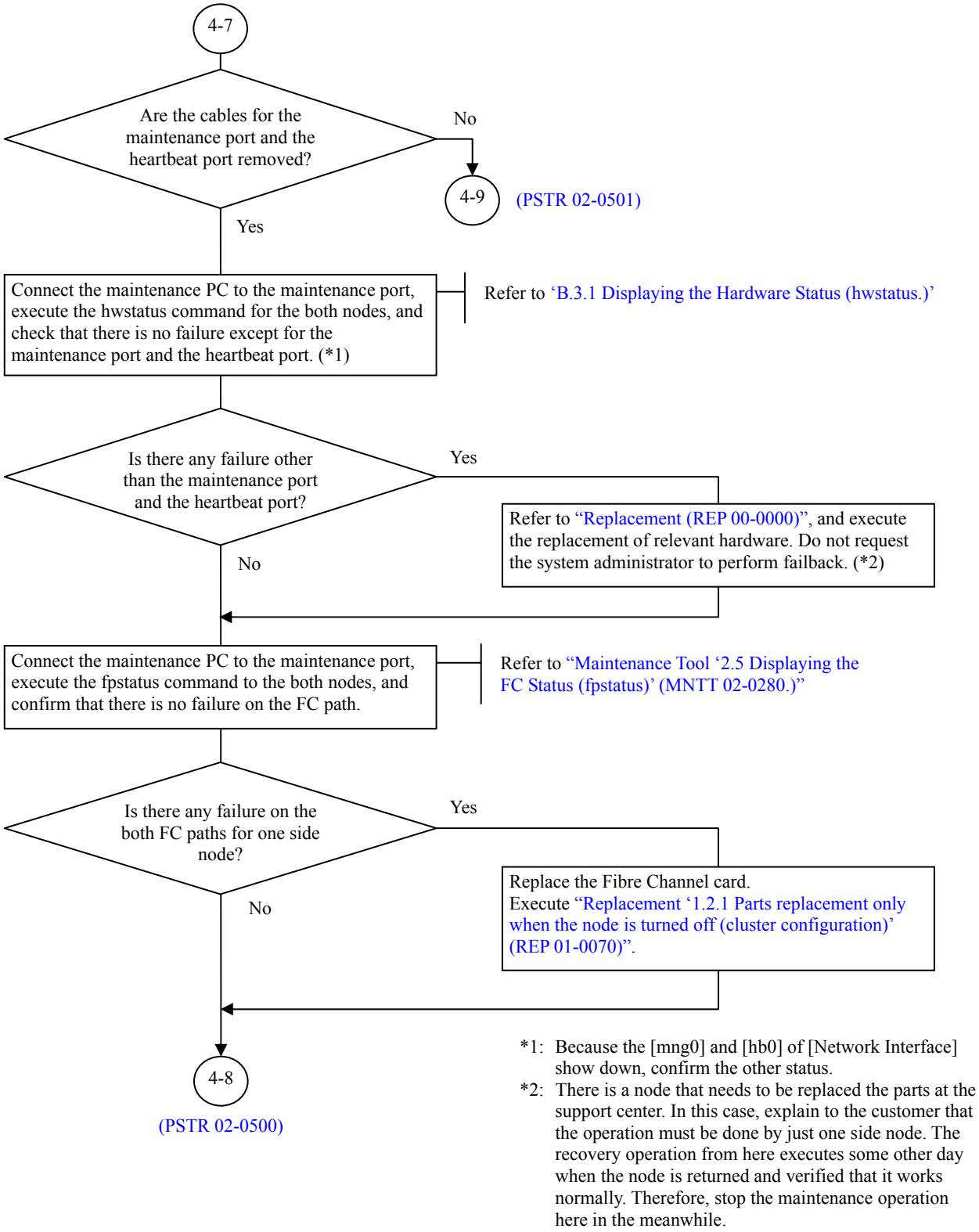
*2: If the system administrator cannot execute the operation, maintenance personnel execute it under the system administrator’s permission. For the execution of failover when the resource group is in operation, refer to “Maintenance Tool ‘2.54 Changing Resource group Execution node (rgmove)’ (MNTT 02-3020)”.

*3: There is a node that needs to be replaced the parts at the support center. In this case, explain to the customer that the operation must be done by just one side node. The recovery operation from here executes some other day when the node is returned and verified that it works normally. Therefore, stop the maintenance operation here in the meanwhile.

*4: Because the OS cannot startup, execute the procedure until just before the startup of OS when the node is returned.

Figure C.2.3.2.2-4 Flow of Management Network Failure Determination (6/9)

Copyright © 2011, 2015, Hitachi, Ltd.

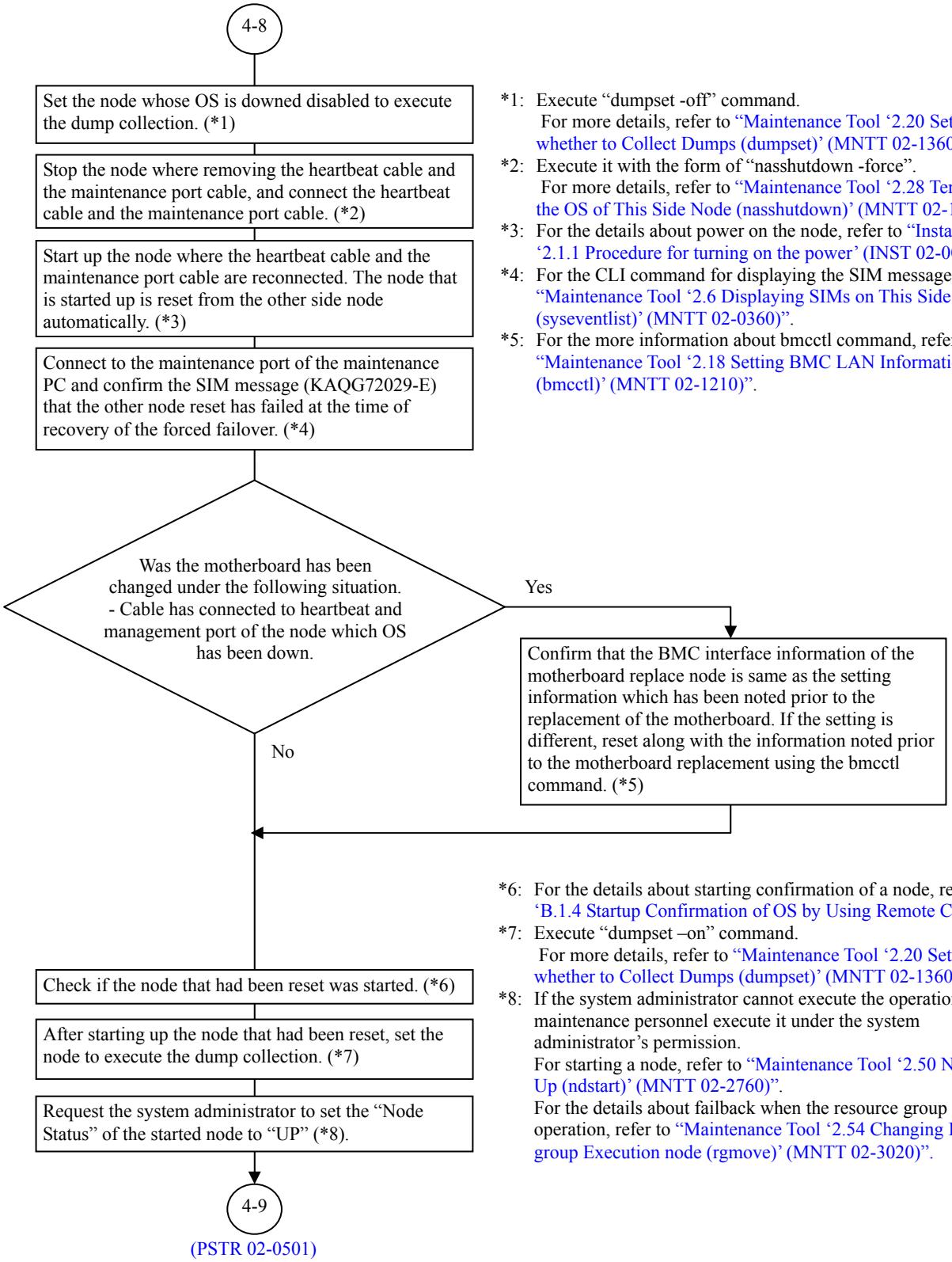


*1: Because the [mng0] and [hb0] of [Network Interface] show down, confirm the other status.

*2: There is a node that needs to be replaced the parts at the support center. In this case, explain to the customer that the operation must be done by just one side node. The recovery operation from here executes some other day when the node is returned and verified that it works normally. Therefore, stop the maintenance operation here in the meanwhile.

Figure C.2.3.2.2-4 Flow of Management Network Failure Determination (7/9)

Copyright © 2011, 2013, Hitachi, Ltd.



*1: Execute "dumpset -off" command.
For more details, refer to "Maintenance Tool '2.20 Setting whether to Collect Dumps (dumpset)' (MNTT 02-1360)".

*2: Execute it with the form of "nasshutdown -force".
For more details, refer to "Maintenance Tool '2.28 Terminating the OS of This Side Node (nasshutdown)' (MNTT 02-1740)".

*3: For the details about power on the node, refer to "Installation '2.1.1 Procedure for turning on the power' (INST 02-0000)".

*4: For the CLI command for displaying the SIM message, refer to "Maintenance Tool '2.6 Displaying SIMs on This Side (syseventlist)' (MNTT 02-0360)".

*5: For the more information about bmcctl command, refer to "Maintenance Tool '2.18 Setting BMC LAN Information (bmcctl)' (MNTT 02-1210)".

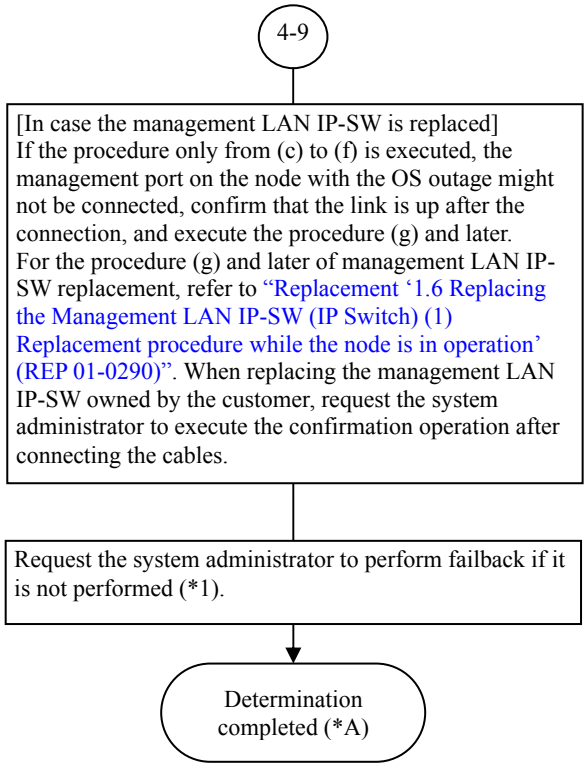
*6: For the details about starting confirmation of a node, refer to 'B.1.4 Startup Confirmation of OS by Using Remote Console'.

*7: Execute "dumpset –on" command.
For more details, refer to "Maintenance Tool '2.20 Setting whether to Collect Dumps (dumpset)' (MNTT 02-1360.)"

*8: If the system administrator cannot execute the operation, maintenance personnel execute it under the system administrator's permission.
For starting a node, refer to "Maintenance Tool '2.50 Node Start Up (ndstart)' (MNTT 02-2760)".
For the details about failback when the resource group is in operation, refer to "Maintenance Tool '2.54 Changing Resource group Execution node (rgmove)' (MNTT 02-3020)".

Figure C.2.3.2.2-4 Flow of Management Network Failure Determination (8/9)

Copyright © 2011, 2013, Hitachi, Ltd.



*1: If the system administrator cannot execute the operation, maintenance personnel execute it under the system administrator's permission.
For starting a node, refer to "Maintenance Tool '2.50 Node Start Up (ndstart)' (MNTT 02-2760)".
For the details about failback when the resource group is in operation, refer to "Maintenance Tool '2.54 Changing Resource group Execution node (rgmove)' (MNTT 02-3020)".

*A: After completing determination, return to 'C.2.2.1 Failure determination procedure at the cluster configuration'.

Figure C.2.3.2.2-4 Flow of Management Network Failure Determination (9/9)

Copyright © 2013, Hitachi, Ltd.

(5) Failure in the BMC port and in the management port of the other node

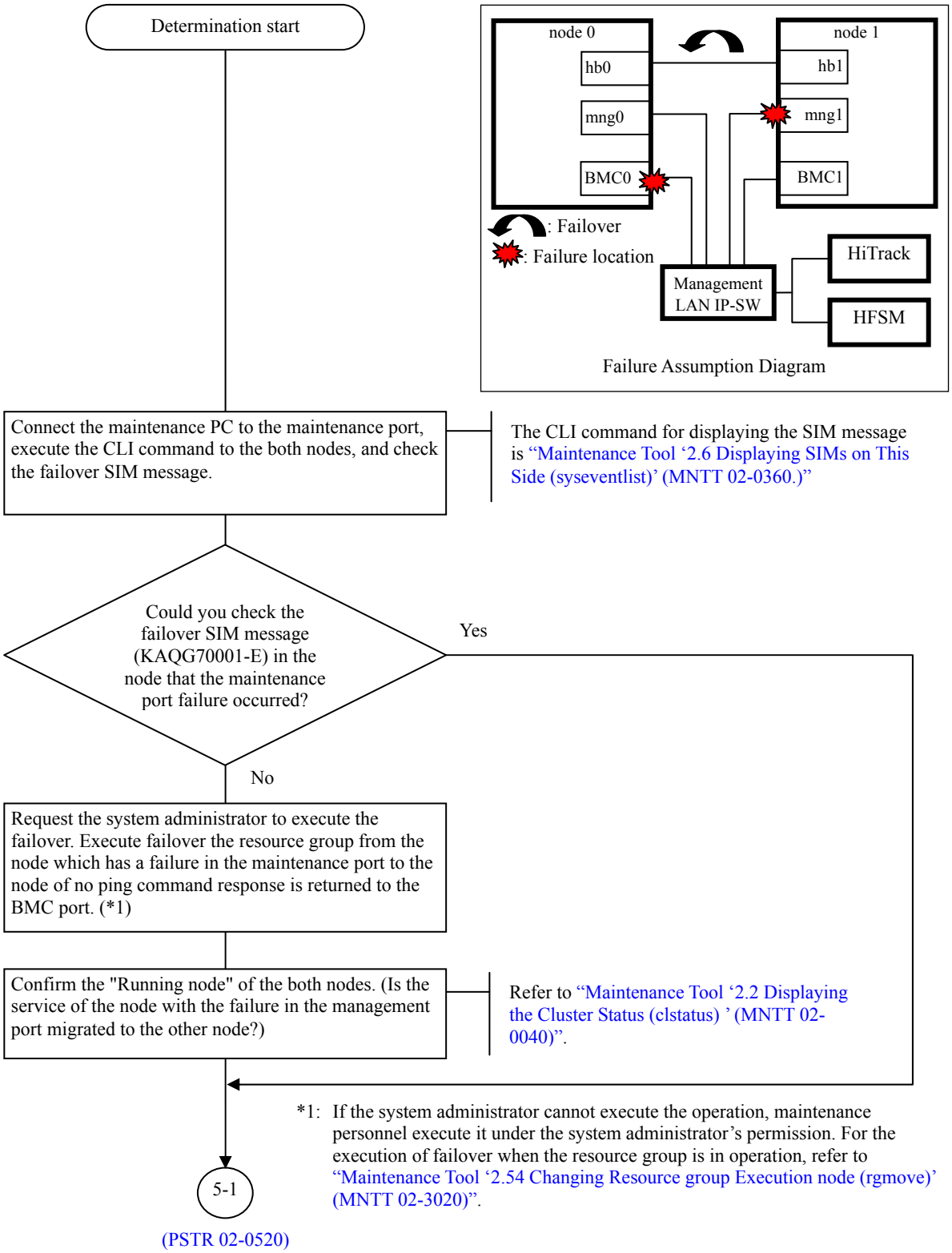


Figure C.2.3.2.2-5 Flow of Management Network Failure Determination (1/6)

Copyright © 2011, 2015, Hitachi, Ltd.

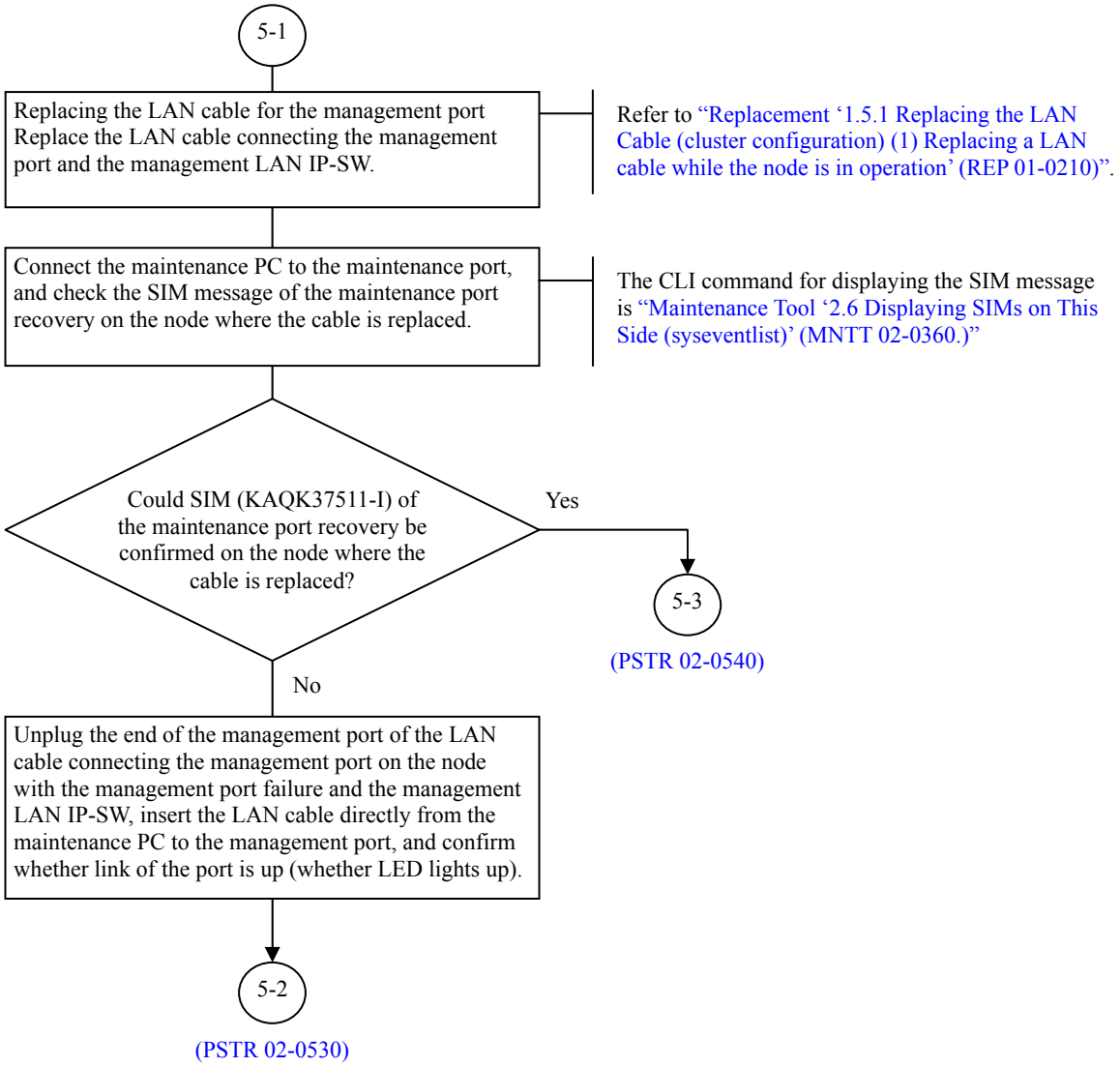
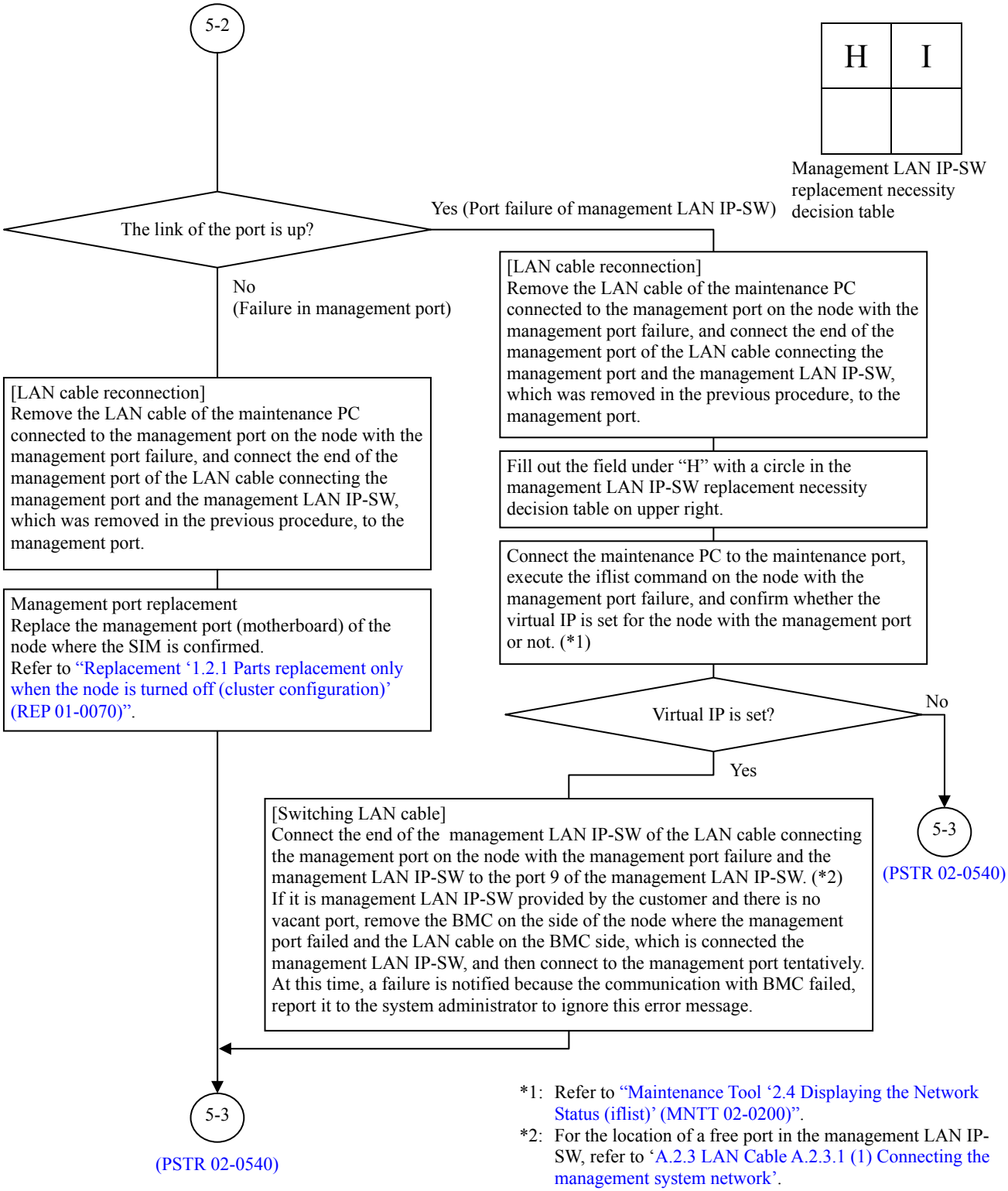


Figure C.2.3.2.2-5 Flow of Management Network Failure Determination (2/6)

Copyright © 2011, 2013, Hitachi, Ltd.



*1: Refer to "Maintenance Tool '2.4 Displaying the Network Status (iflist)' (MNTT 02-0200)".

*2: For the location of a free port in the management LAN IP-SW, refer to 'A.2.3 LAN Cable A.2.3.1 (1) Connecting the management system network'.

Figure C.2.3.2.2-5 Flow of Management Network Failure Determination (3/6)

Copyright © 2011, 2014, Hitachi, Ltd.

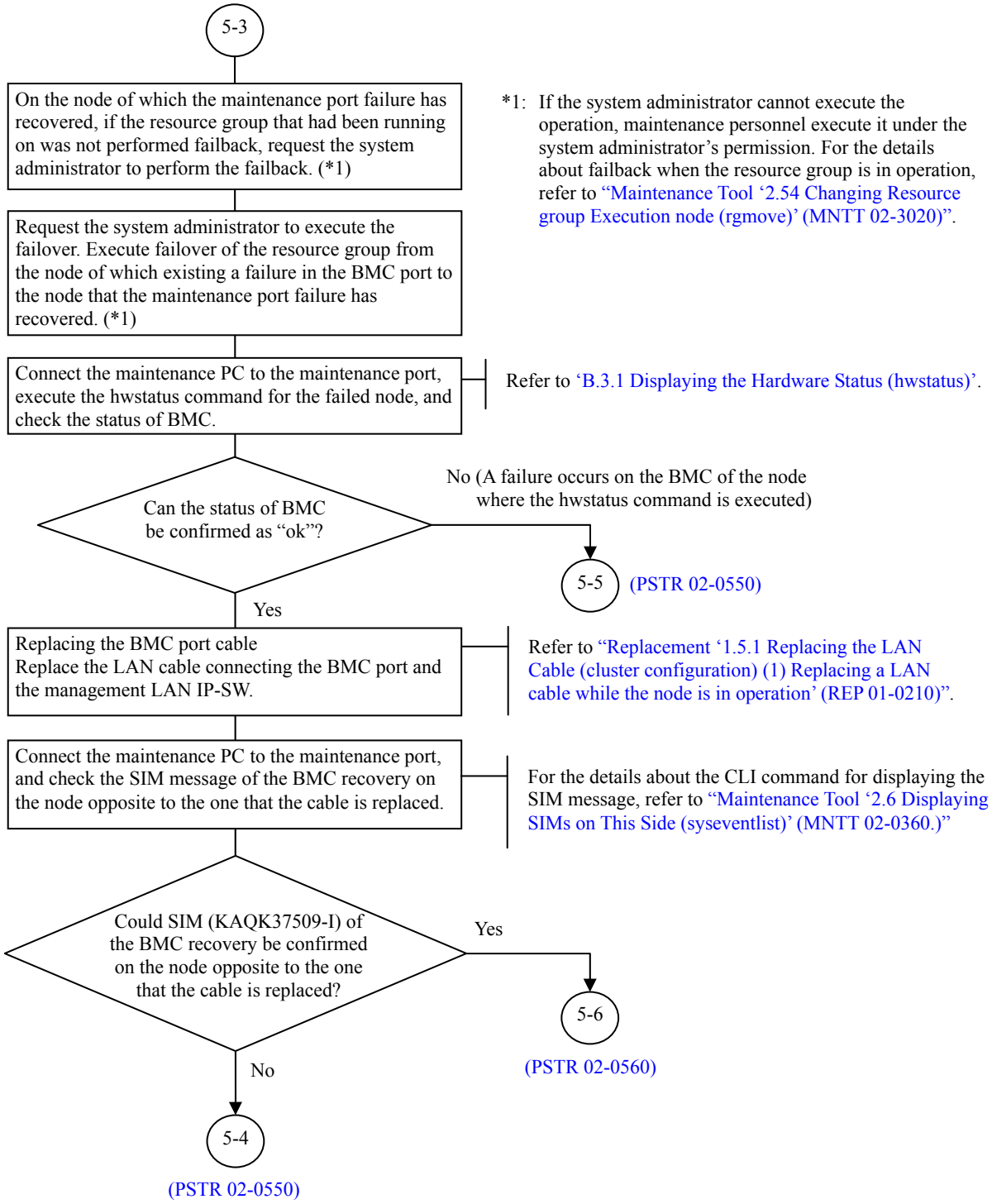


Figure C.2.3.2.2-5 Flow of Management Network Failure Determination (4/6)

Copyright © 2011, 2013, Hitachi, Ltd.

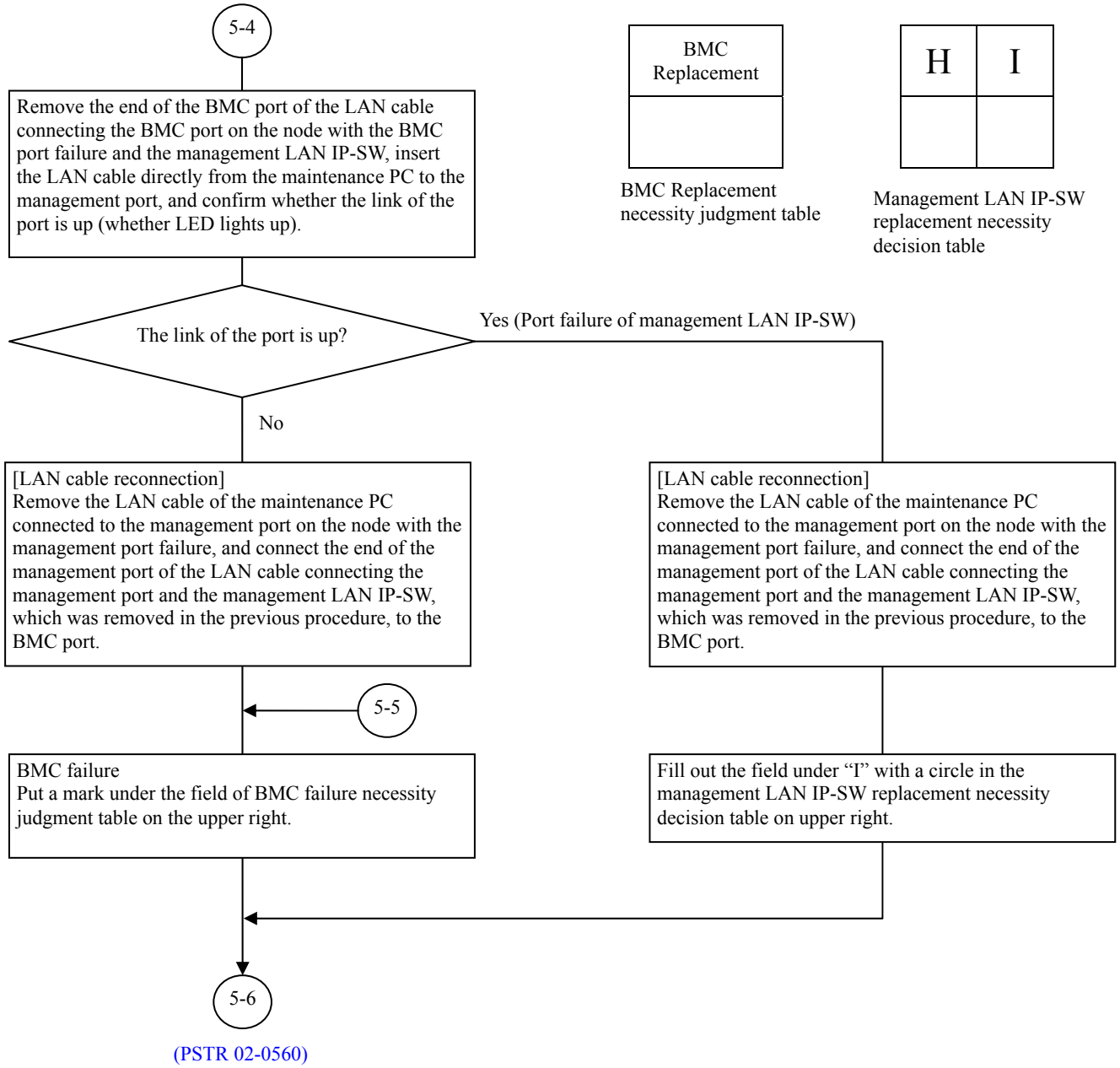
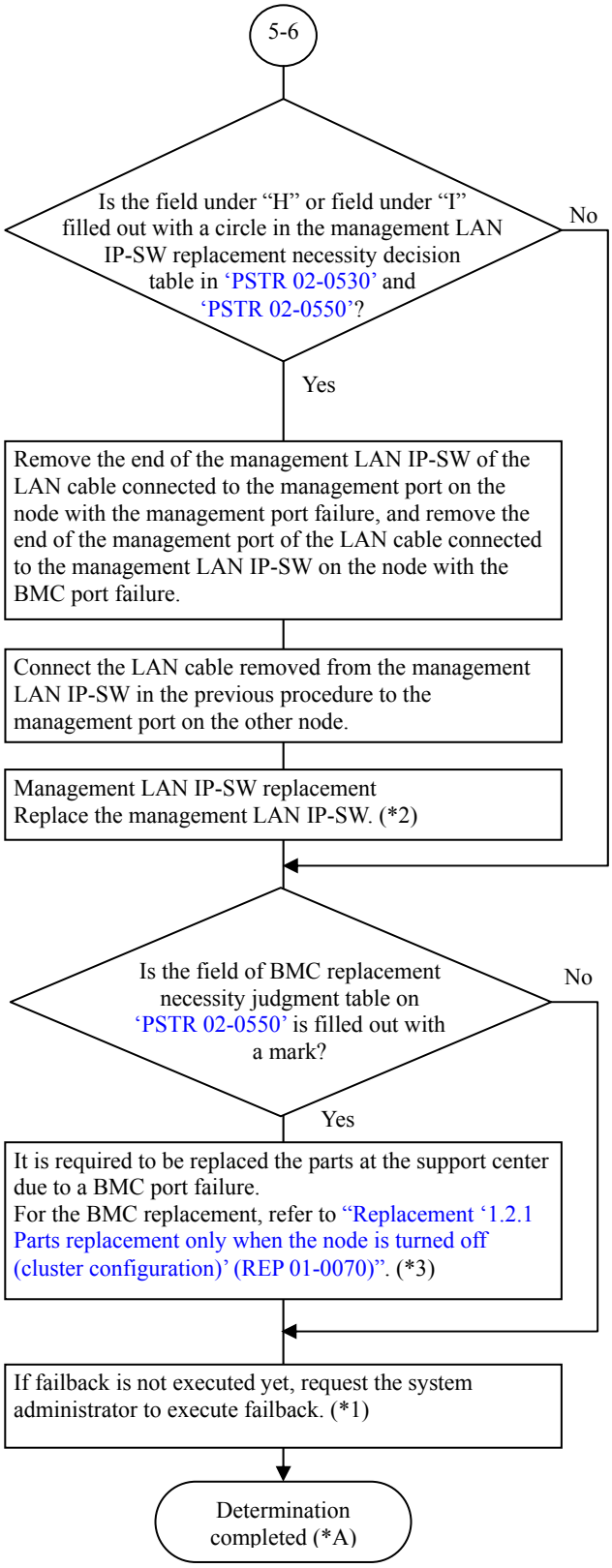


Figure C.2.3.2.2-5 Flow of Management Network Failure Determination (5/6)

Copyright © 2011, 2014, Hitachi, Ltd.



*1: If the system administrator cannot execute the operation, maintenance personnel execute it under the system administrator's permission. For the details about failback when the resource group is in operation, refer to "Maintenance Tool '2.54 Changing Resource group Execution node (rgmove)' (MNTT 02-3020)".

*2: Refer to "Replacement '1.6 Replacing the Management LAN IP-SW (IP Switch) (1) Replacement procedure while the node is in operation' (REP 01-0290)".
If it is the management LAN IP-SW owned by the customer, request the customer to replace the management LAN IP-SW. The maintenance personnel should execute the rest of the operation after the report that the replacement is completed.

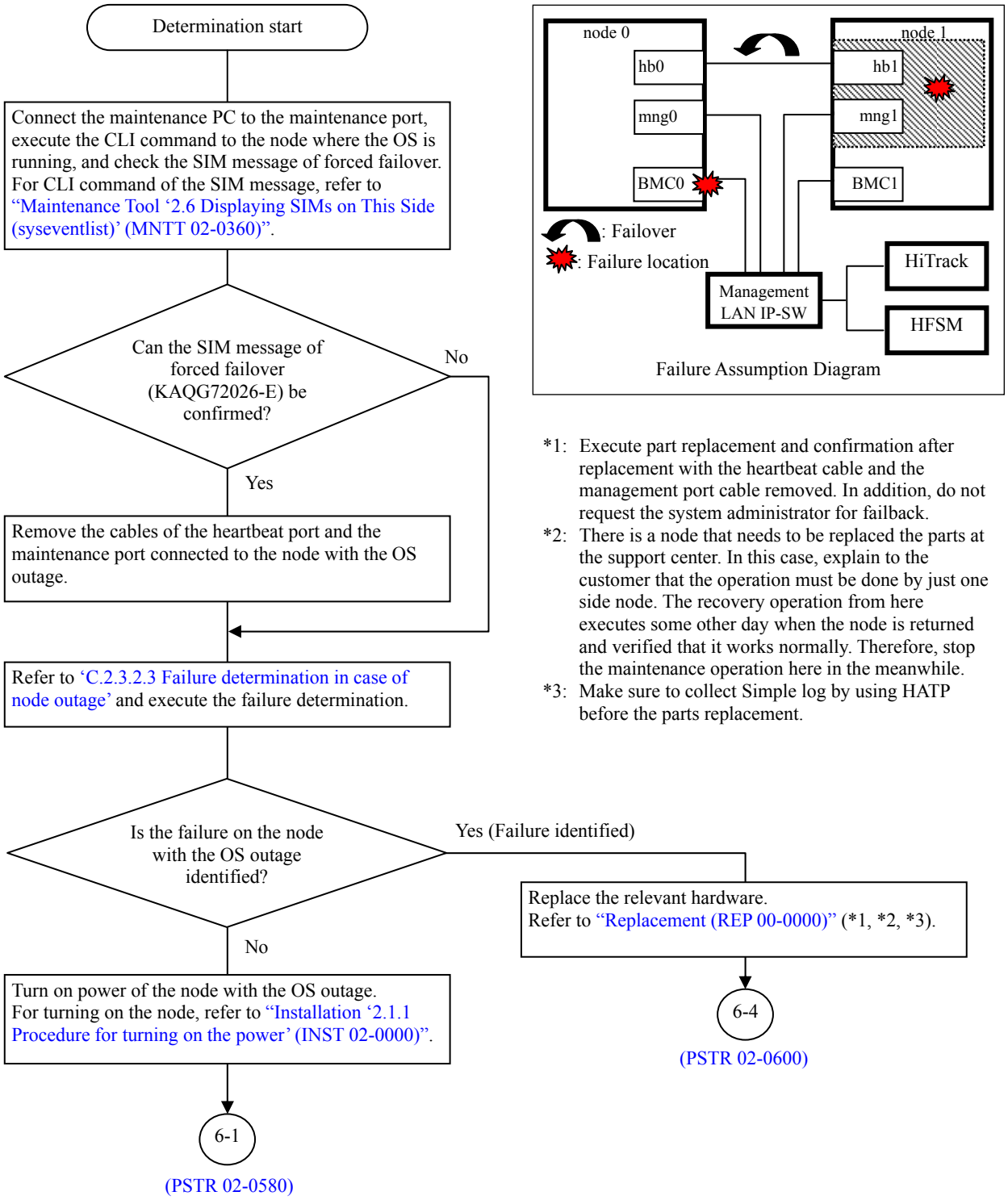
*3: There is a node that needs to be replaced the parts at the support center. In this case, explain to the customer that the operation must be done by just one side node. The recovery operation from here executes some other day when the node is returned and verified that it works normally. Therefore, stop the maintenance operation here in the meanwhile.

*A: After completing determination, return to 'C.2.2.1 Failure determination procedure at the cluster configuration'.

Figure C.2.3.2.2-5 Flow of Management Network Failure Determination (6/6)

Copyright © 2011, 2014, Hitachi, Ltd.

(6) OS down and a failure in the BMC port of the other node



*1: Execute part replacement and confirmation after replacement with the heartbeat cable and the management port cable removed. In addition, do not request the system administrator for failback.

*2: There is a node that needs to be replaced the parts at the support center. In this case, explain to the customer that the operation must be done by just one side node. The recovery operation from here executes some other day when the node is returned and verified that it works normally. Therefore, stop the maintenance operation here in the meanwhile.

*3: Make sure to collect Simple log by using HATP before the parts replacement.

Figure C.2.3.2.2-6 Flow of Management Network Failure Determination (1/5)

Copyright © 2011, 2015, Hitachi, Ltd.

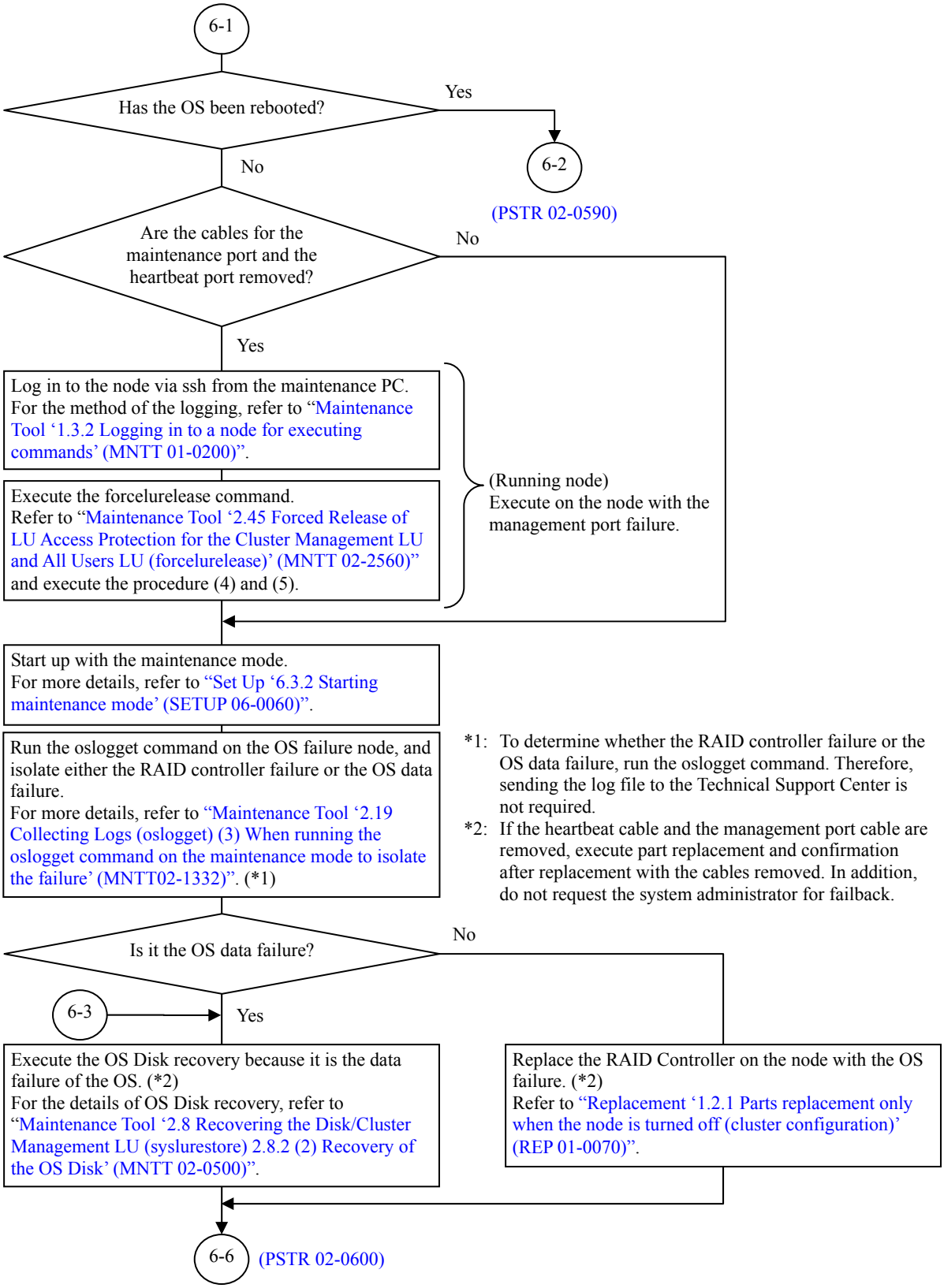
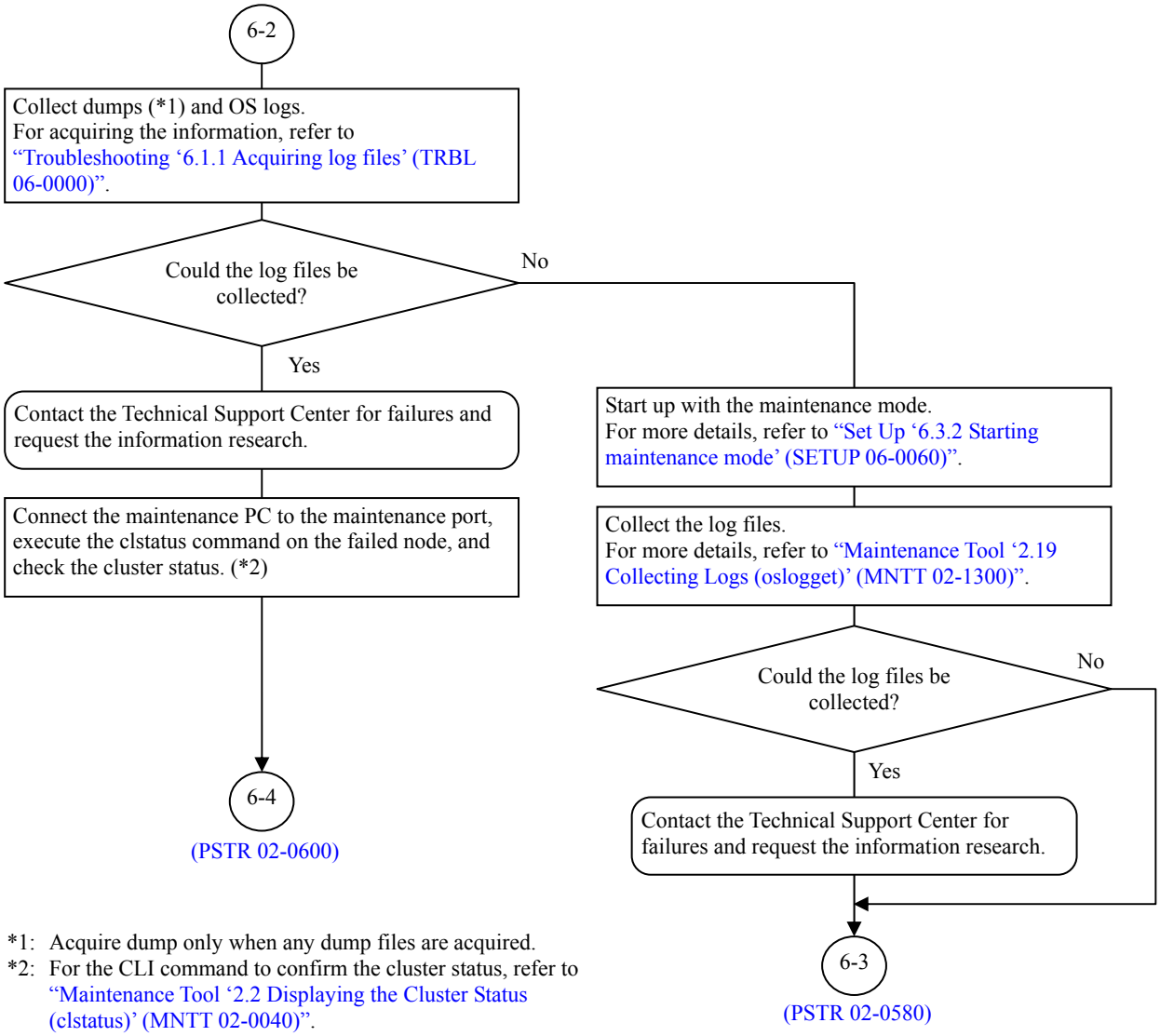


Figure C.2.3.2.2-6 Flow of Management Network Failure Determination (2/5)

Copyright © 2011, 2015, Hitachi, Ltd.



*1: Acquire dump only when any dump files are acquired.
*2: For the CLI command to confirm the cluster status, refer to "Maintenance Tool '2.2 Displaying the Cluster Status (clstatus)' (MNTT 02-0040)".

Figure C.2.3.2.2-6 Flow of Management Network Failure Determination (3/5)

Copyright © 2011, 2013, Hitachi, Ltd.

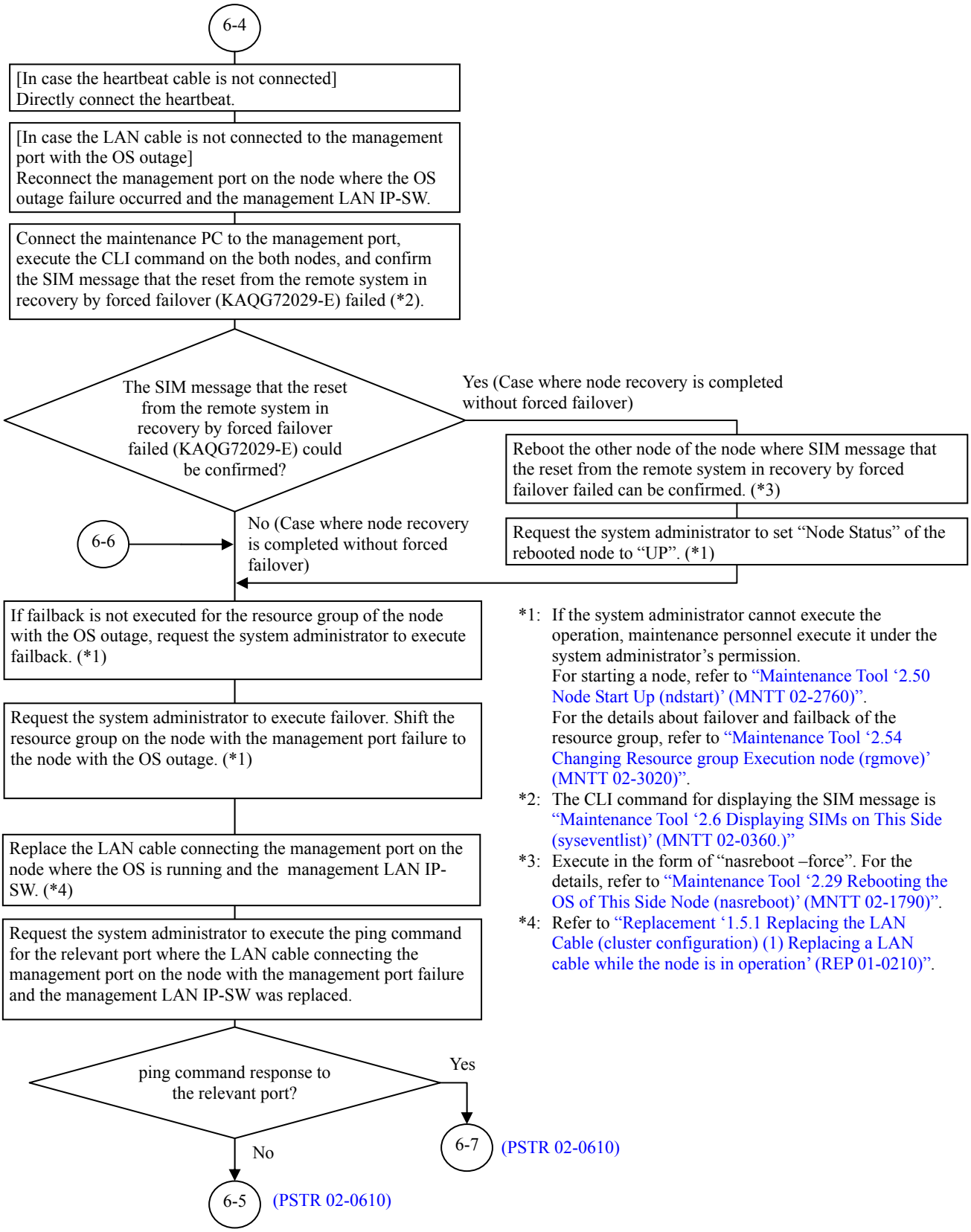


Figure C.2.3.2.2-6 Flow of Management Network Failure Determination (4/5)

Copyright © 2011, 2014, Hitachi, Ltd.

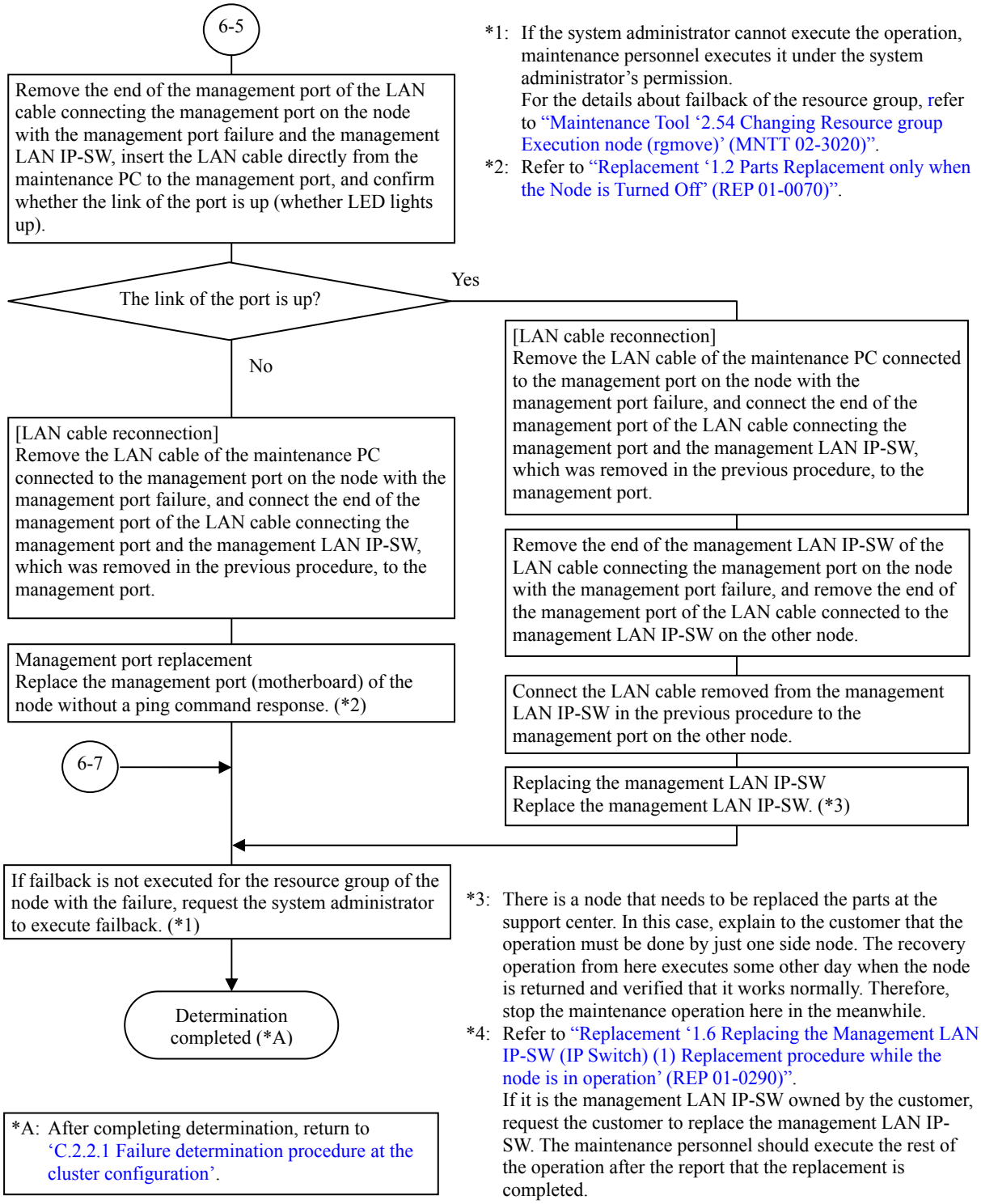


Figure C.2.3.2.2-6 Flow of Management Network Failure Determination (5/5)

Copyright © 2011, 2013, Hitachi, Ltd.

(7) Failure in the management ports of the both nodes

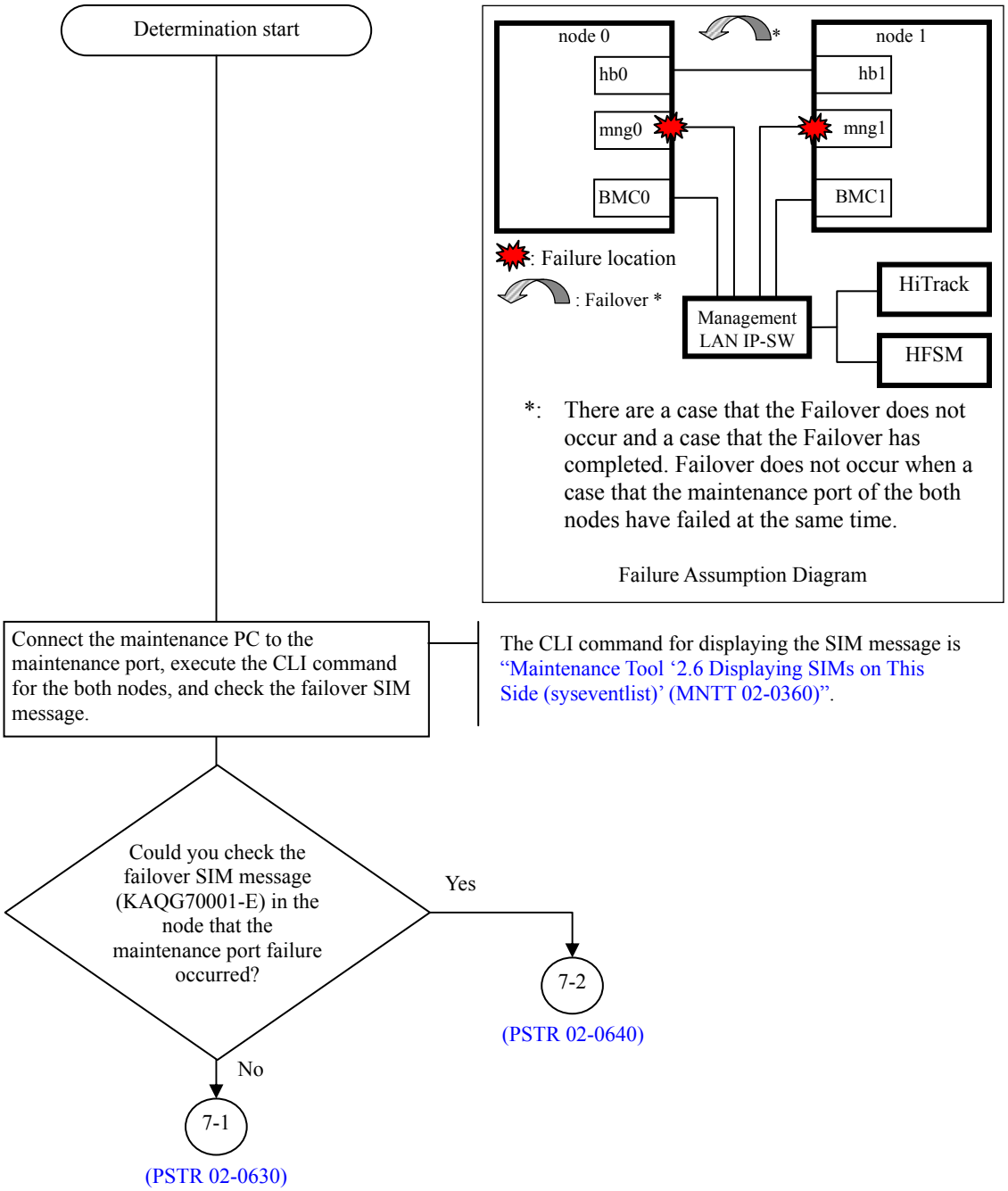
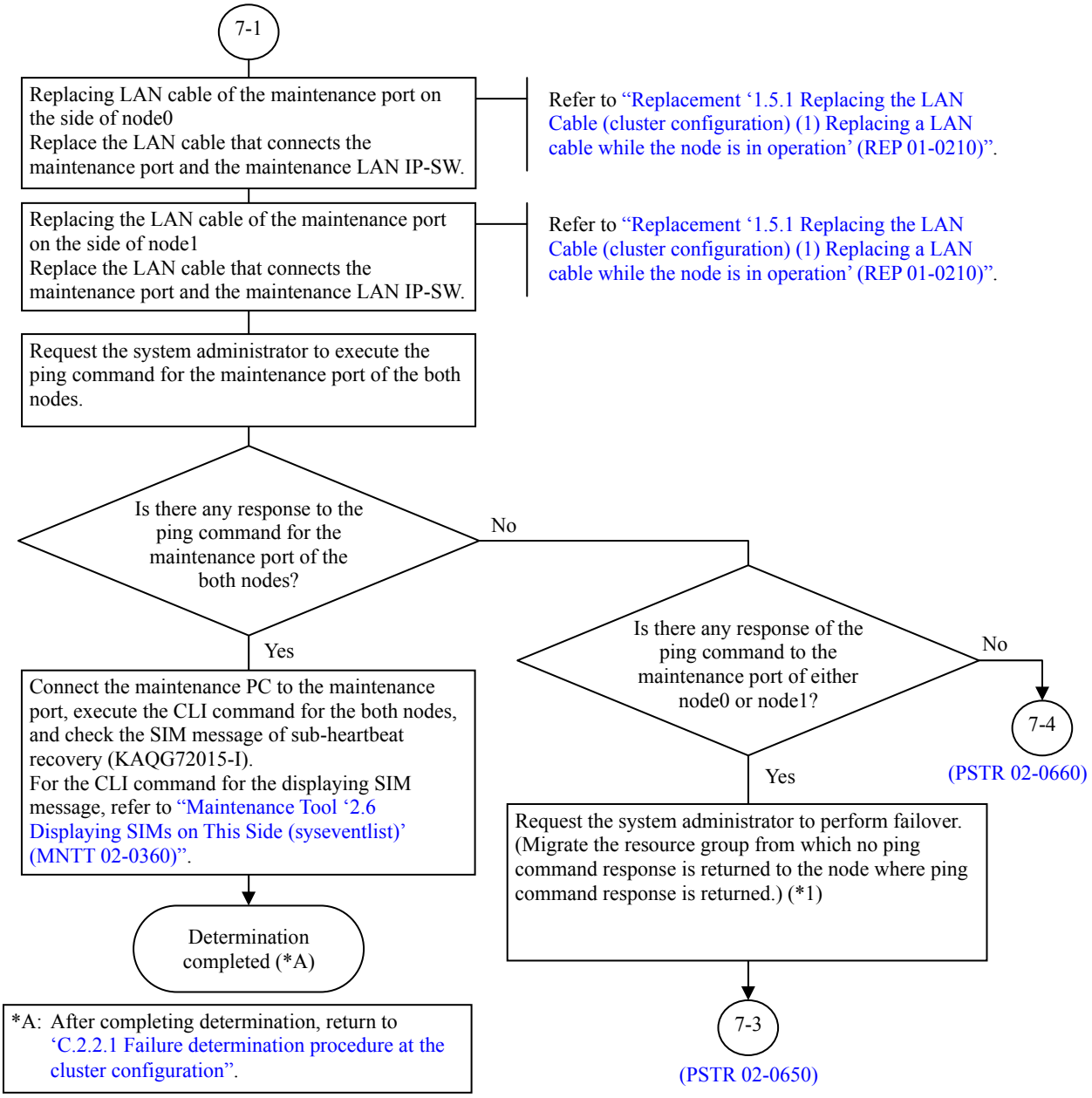


Figure C.2.3.2.2-7 Flow of Management Network Failure Determination (1/11)

Copyright © 2011, 2015, Hitachi, Ltd.



*1: If the system administrator cannot execute the operation, maintenance personnel execute it under the system administrator's permission. For the execution of failover when the resource group is in operation, refer to "Maintenance Tool '2.54 Changing Resource group Execution node (rgmove)' (MNTT 02-3020)".

Figure C.2.3.2.2-7 Flow of Management Network Failure Determination (2/11)

Copyright © 2011, 2013, Hitachi, Ltd.

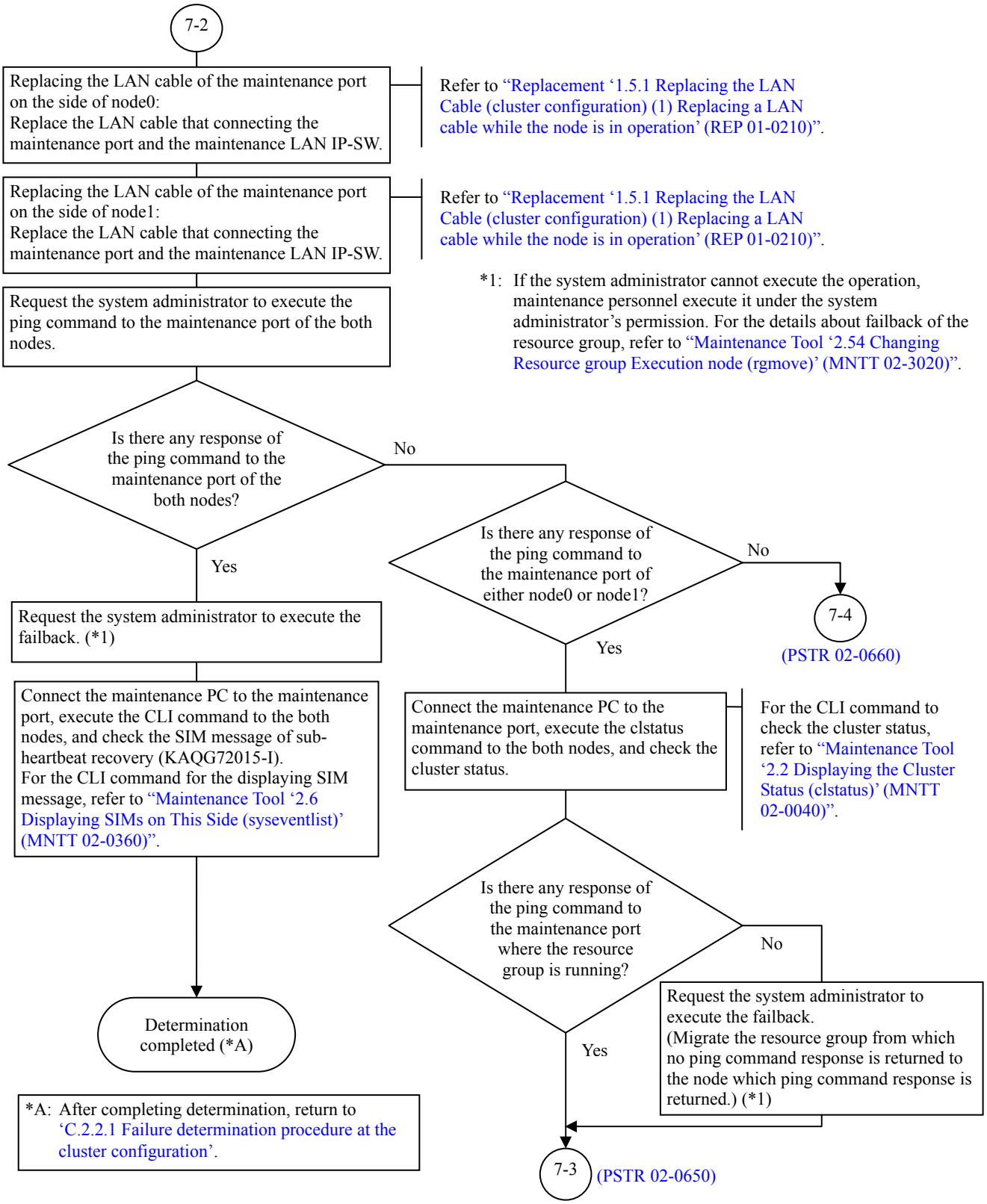
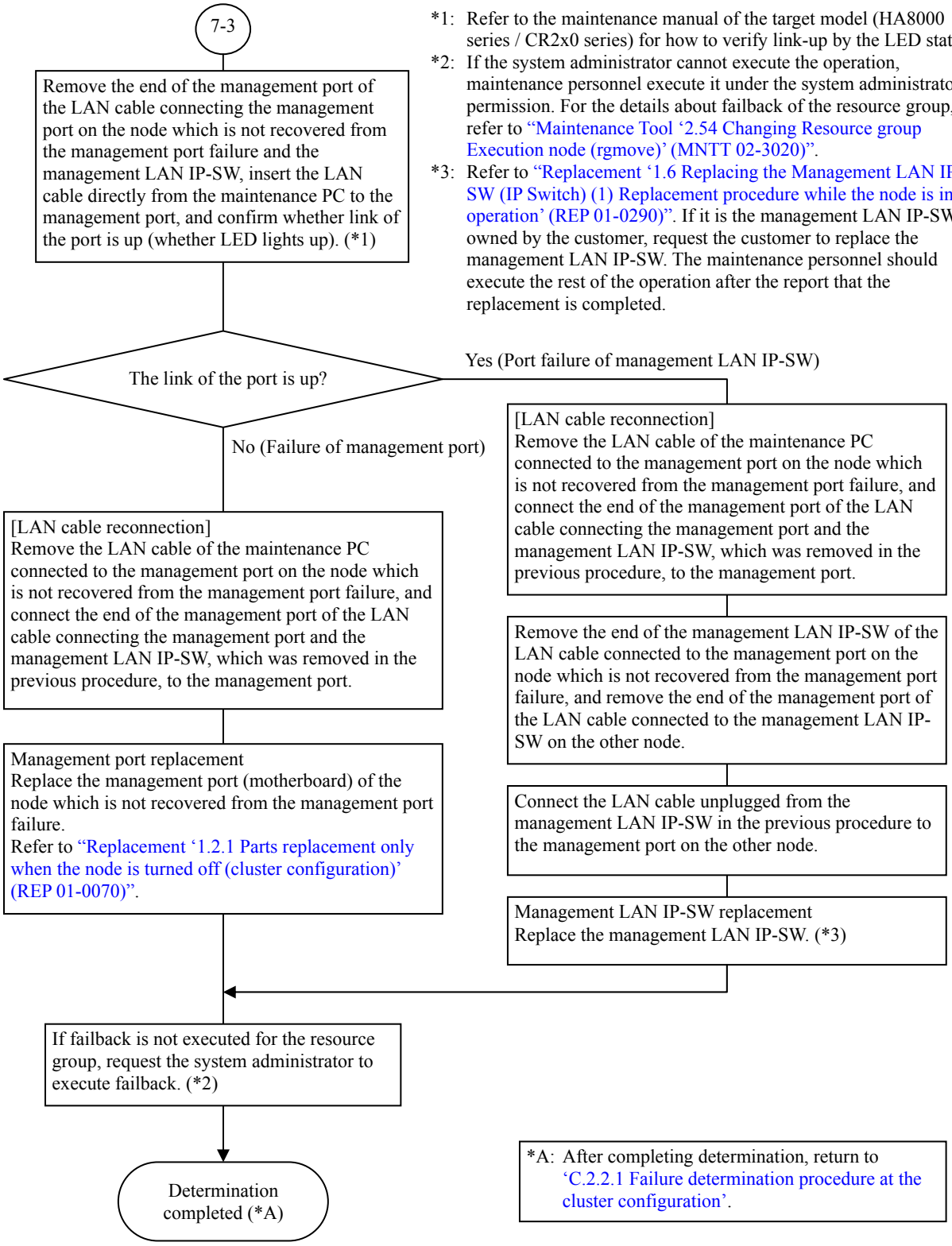


Figure C.2.3.2.2-7 Flow of Management Network Failure Determination (3/11)

Copyright © 2011, 2013, Hitachi, Ltd.



*1: Refer to the maintenance manual of the target model (HA8000 series / CR2x0 series) for how to verify link-up by the LED status.

*2: If the system administrator cannot execute the operation, maintenance personnel execute it under the system administrator's permission. For the details about failback of the resource group, refer to "Maintenance Tool '2.54 Changing Resource group Execution node (rgmove)' (MNTT 02-3020)".

*3: Refer to "Replacement '1.6 Replacing the Management LAN IP-SW (IP Switch) (1) Replacement procedure while the node is in operation' (REP 01-0290)". If it is the management LAN IP-SW owned by the customer, request the customer to replace the management LAN IP-SW. The maintenance personnel should execute the rest of the operation after the report that the replacement is completed.

*A: After completing determination, return to 'C.2.2.1 Failure determination procedure at the cluster configuration'.

Figure C.2.3.2.2-7 Flow of Management Network Failure Determination (4/11)

Copyright © 2011, 2015, Hitachi, Ltd.

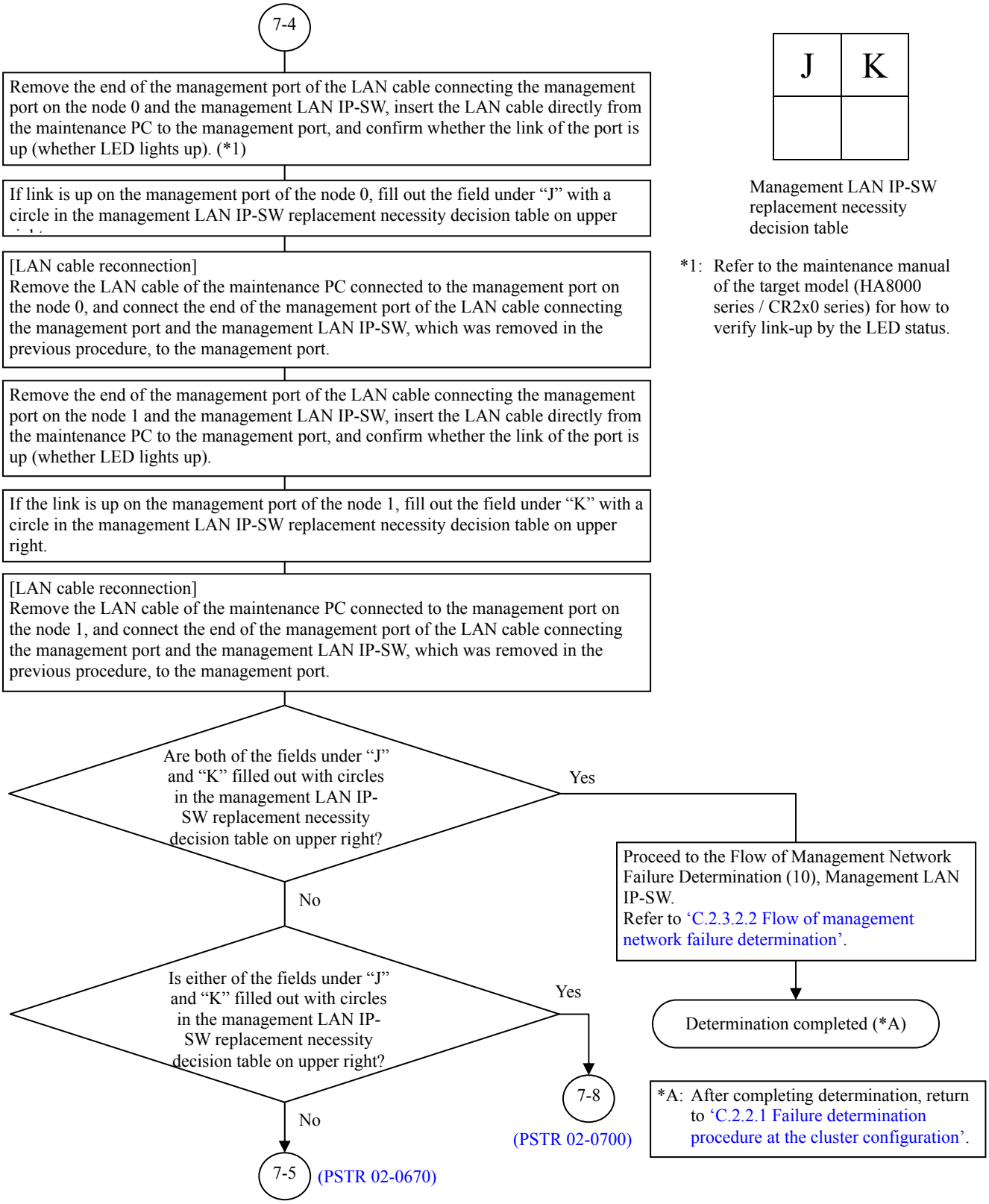
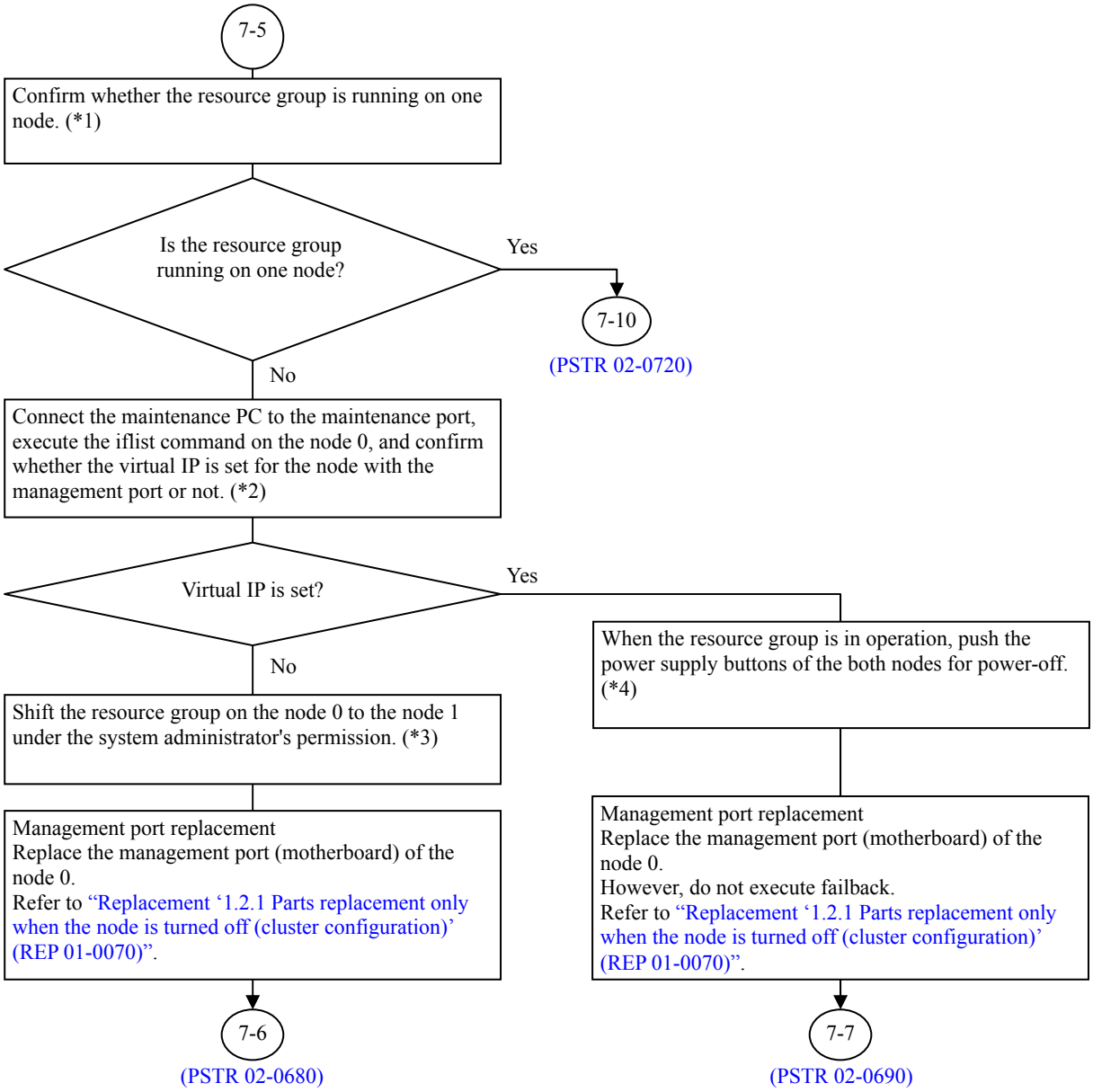


Figure C.2.3.2.2-7 Flow of Management Network Failure Determination (5/11)

Copyright © 2011, 2015, Hitachi, Ltd.



*1: For the confirmation of the resource group, refer to "Maintenance Tool '2.2 Displaying the Cluster Status (clstatus)' (MNTT 02-0040)".
*2: Refer to "Maintenance Tool '2.4 Displaying the Network Status (iflist)' (MNTT 02-0200)".
*3: Maintenance personnel should execute it under the system administrator's permission. For the details about failback of the resource group, refer to "Maintenance Tool '2.54 Changing Resource group Execution node (rgmove)' (MNTT 02-3020)".
*4: Refer to "Installation '2.1.2.2 Terminating the OS of the node by operating the power button' (INST 02-0080)".

Figure C.2.3.2.2-7 Flow of Management Network Failure Determination (6/11)

Copyright © 2011, 2013, Hitachi, Ltd.

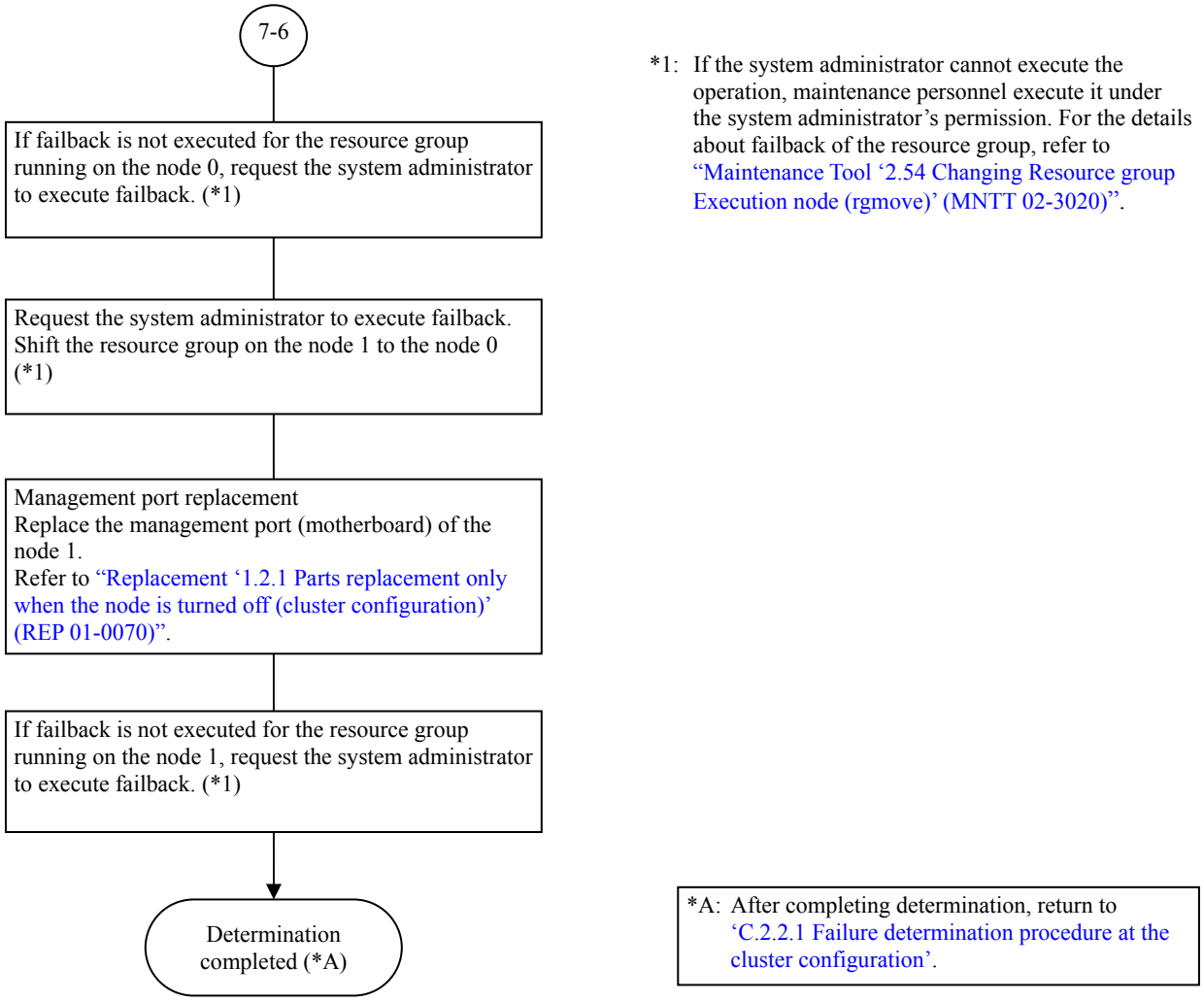


Figure C.2.3.2.2-7 Flow of Management Network Failure Determination (7/11)

Copyright © 2011, 2013, Hitachi, Ltd.

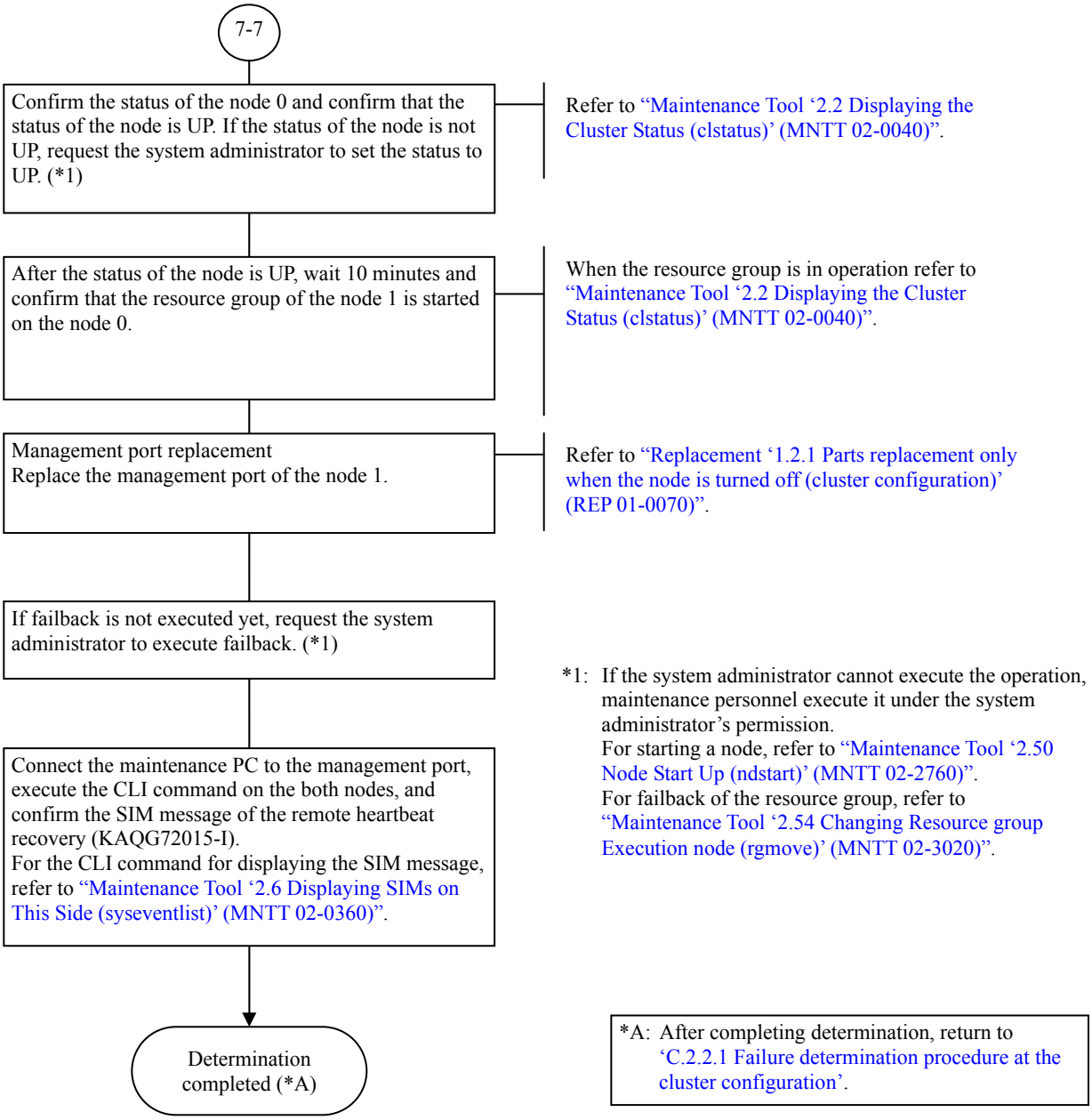
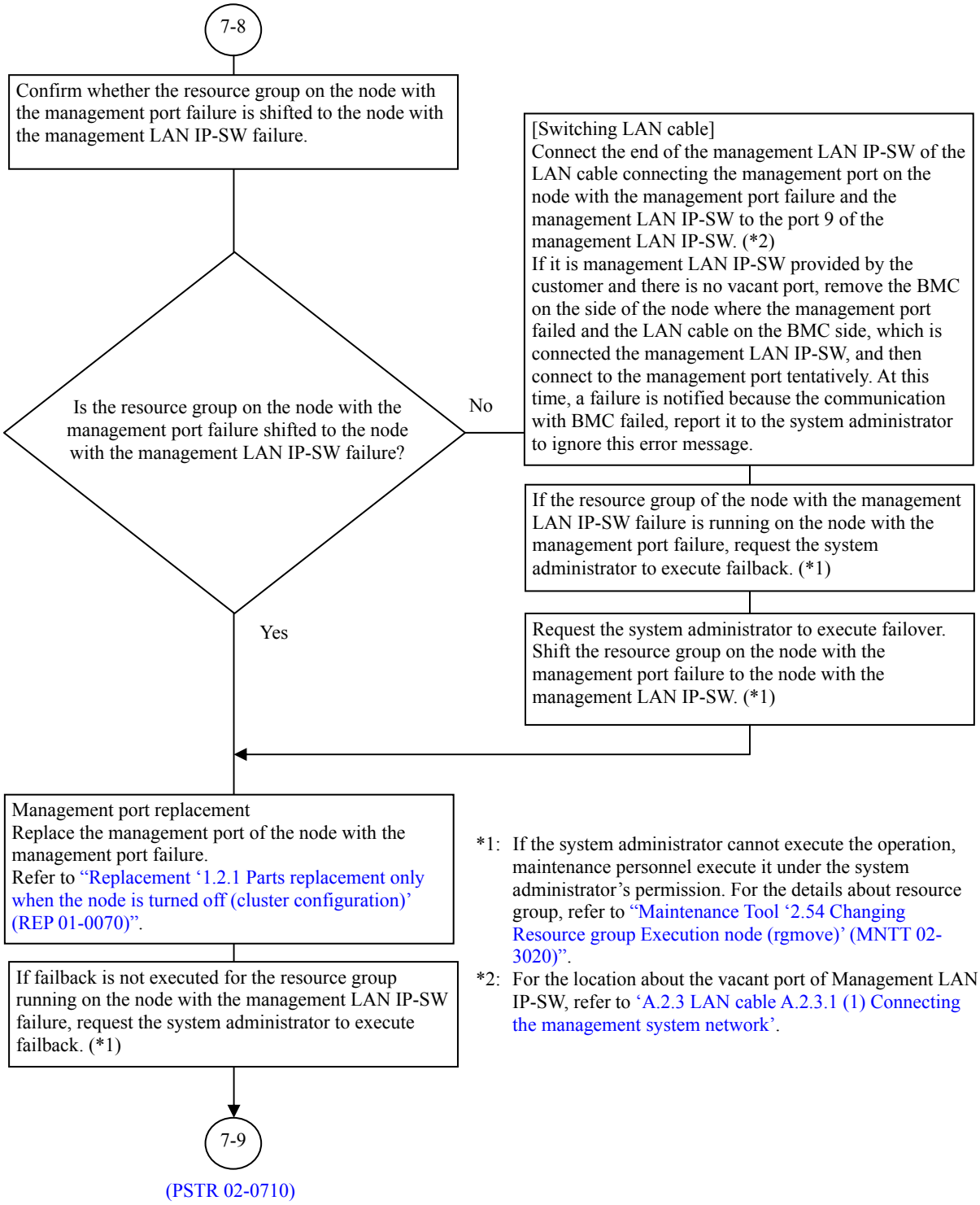


Figure C.2.3.2.2-7 Flow of Management Network Failure Determination (8/11)

Copyright © 2011, 2013, Hitachi, Ltd.

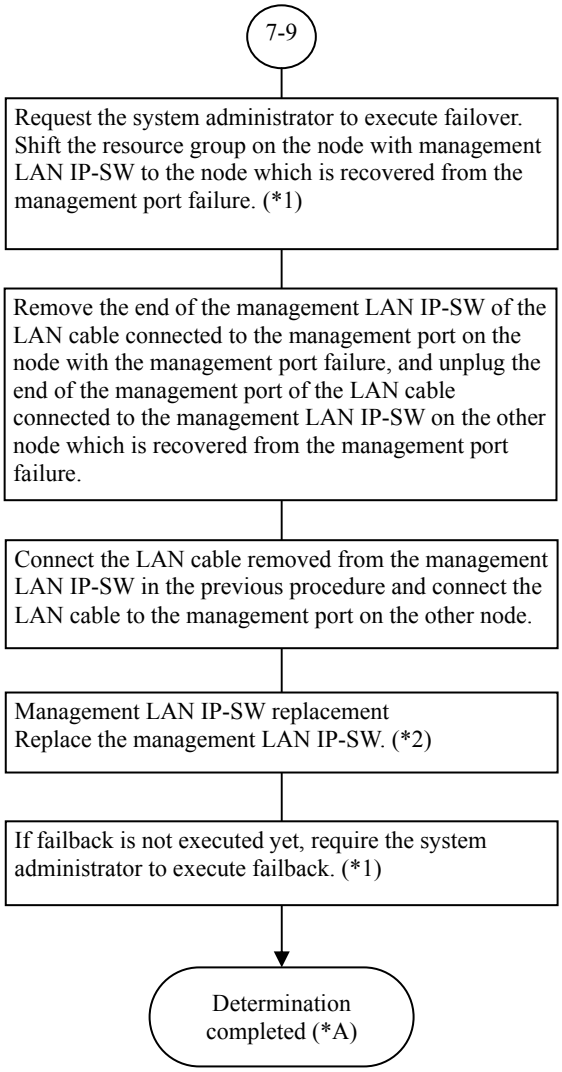


*1: If the system administrator cannot execute the operation, maintenance personnel execute it under the system administrator's permission. For the details about resource group, refer to "Maintenance Tool '2.54 Changing Resource group Execution node (rgmove)' (MNTT 02-3020)".

*2: For the location about the vacant port of Management LAN IP-SW, refer to 'A.2.3 LAN cable A.2.3.1 (1) Connecting the management system network'.

Figure C.2.3.2.2-7 Flow of Management Network Failure Determination (9/11)

Copyright © 2011, 2017, Hitachi, Ltd.



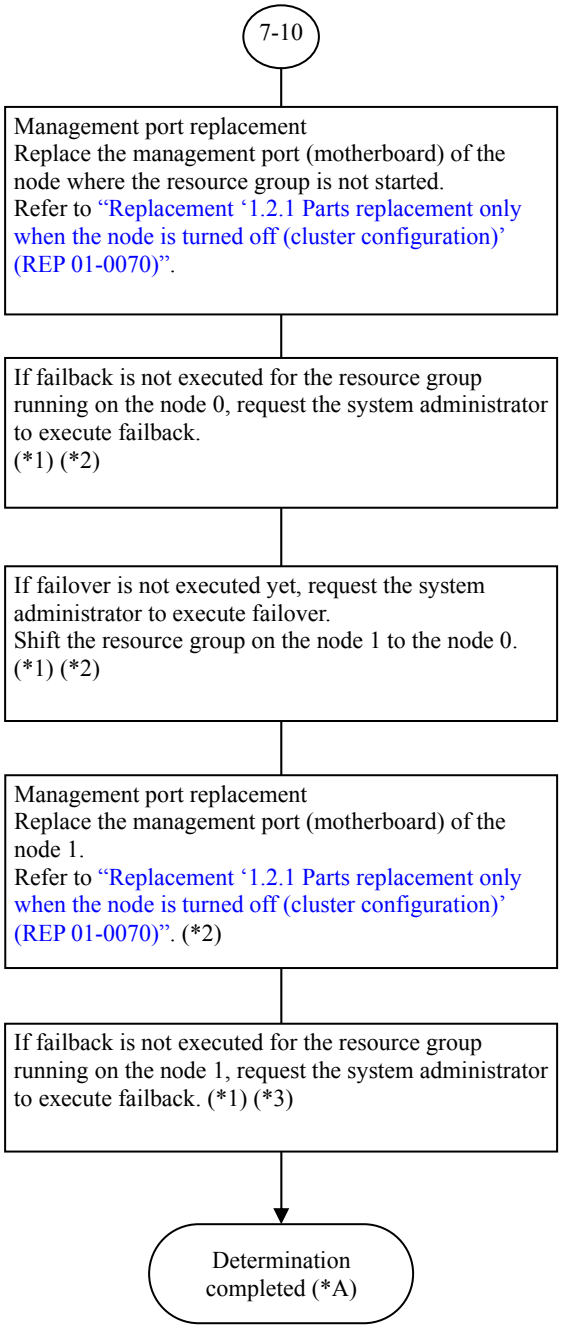
*1: If the system administrator cannot execute the operation, maintenance personnel execute it under the system administrator's permission. For the details about resource group, refer to "Maintenance Tool '2.54 Changing Resource group Execution node (rgmove)' (MNTT 02-3020)".

*2: For the location of a free port in the management LAN IP-SW, refer to "Replacement '1.6 Replacing the Management LAN IP-SW (IP Switch) (1) Replacement procedure while the node is in operation' (REP 01-0290)". If it is the management LAN IP-SW owned by the customer, request the customer to replace the management LAN IP-SW. request the replacement. The maintenance personnel should execute the rest of the operation after the report that the replacement is completed.

*A: After completing determination, return to 'C.2.2.1 Failure determination procedure at the cluster configuration'.

Figure C.2.3.2.2-7 Flow of Management Network Failure Determination (10/11)

Copyright © 2011, 2013, Hitachi, Ltd.



*1: If the system administrator cannot execute the operation, maintenance personnel execute it under the system administrator's permission. For the details about resource group, refer to "Maintenance Tool '2.54 Changing Resource group Execution node (rgmove)' (MNTT 02-3020)".

*2: If the management port on the node 1 is already replaced, read the node 1 as the node 0, and the node 0 as the node 1.

*3: If the management port on the node 0 is replaced in the previous procedure, read the node 1 as the node 0.

*A: After completing determination, return to 'C.2.2.1 Failure determination procedure at the cluster configuration'.

Figure C.2.3.2.2-7 Flow of Management Network Failure Determination (11/11)

Copyright © 2011, 2014, Hitachi, Ltd.

(8) Failure in the management port of the other node after the OS down and the failover completion

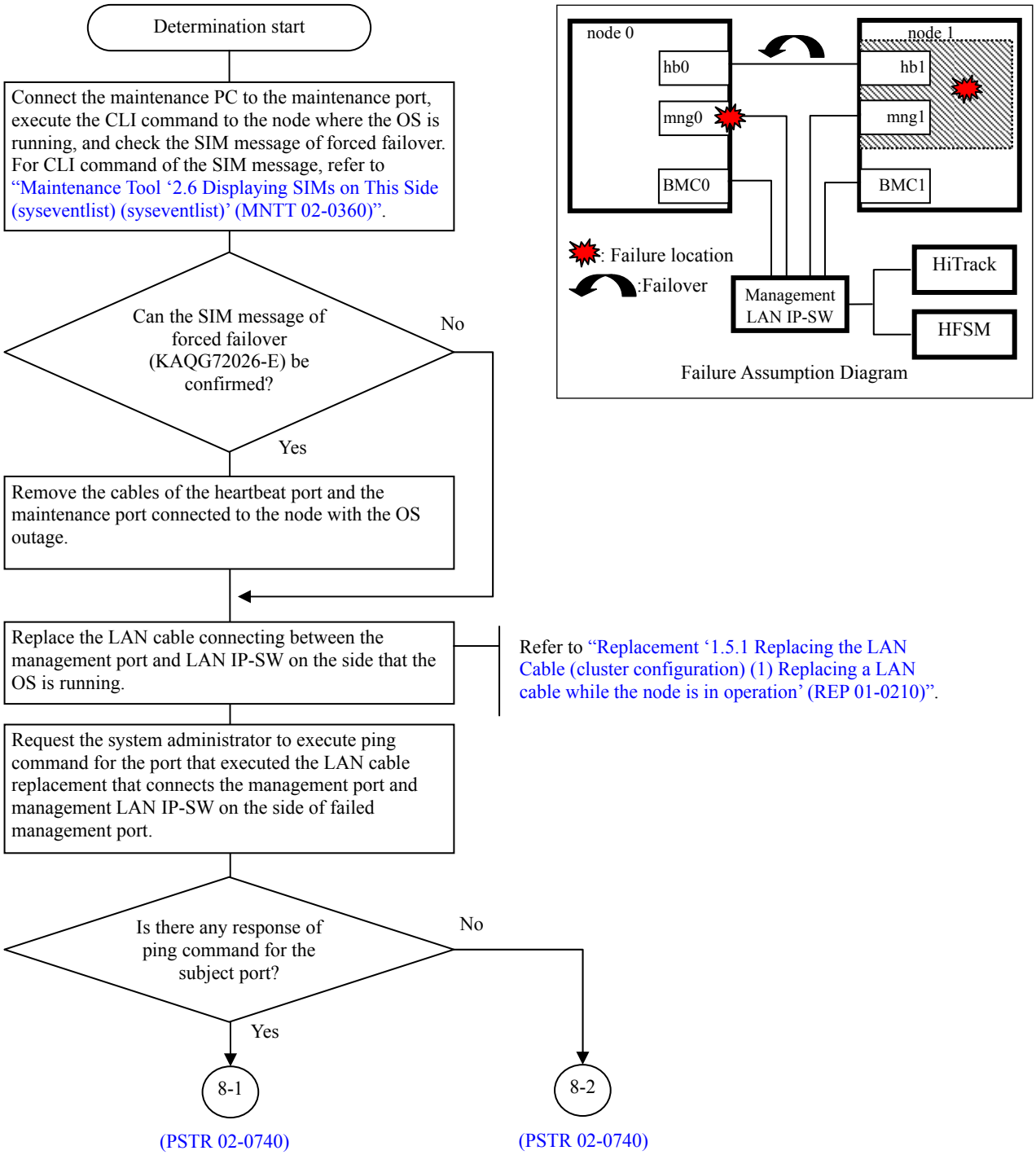
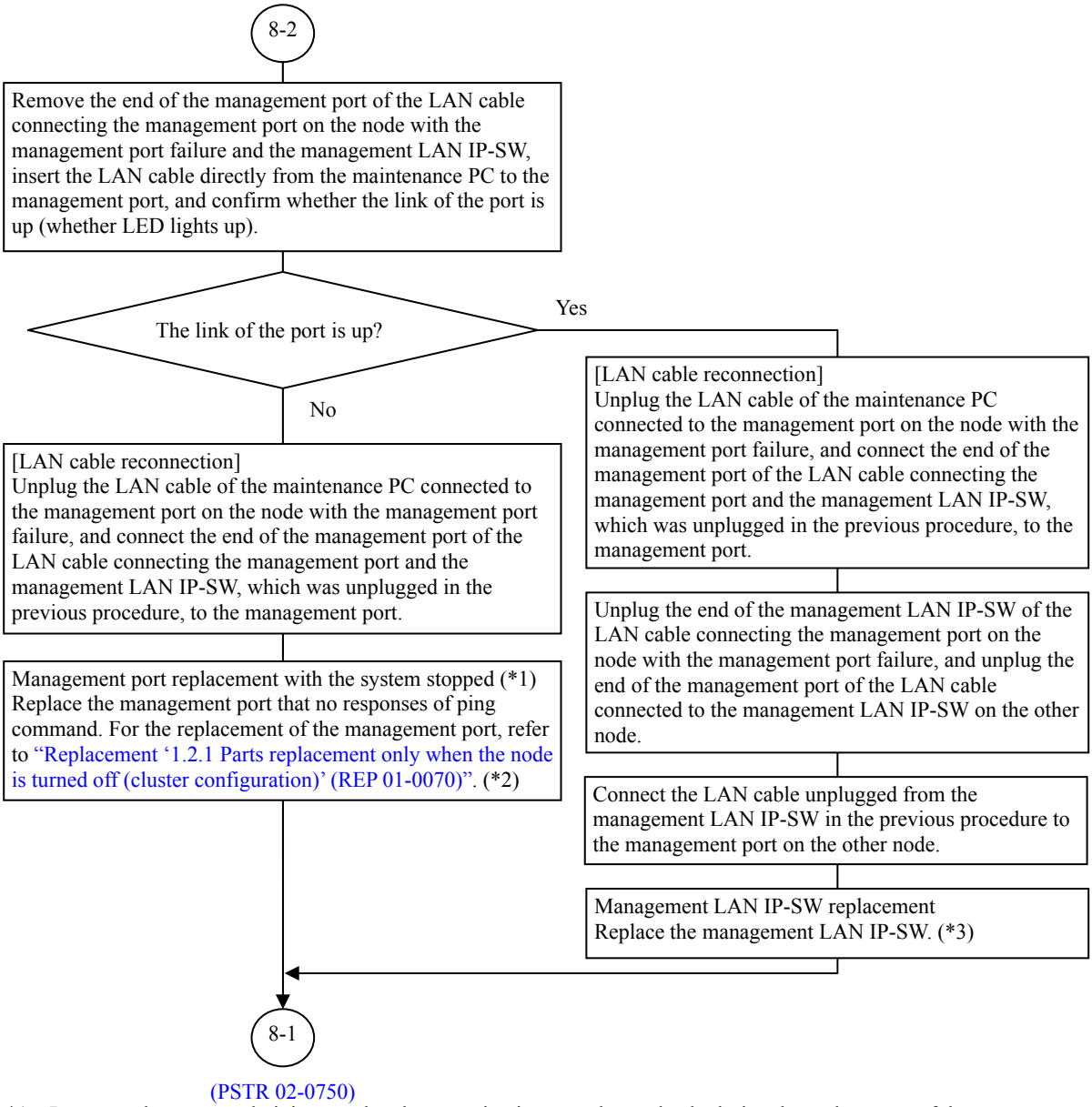


Figure C.2.3.2.2-8 Flow of Management Network Failure Determination (1/6)

Copyright © 2011, 2015, Hitachi, Ltd.



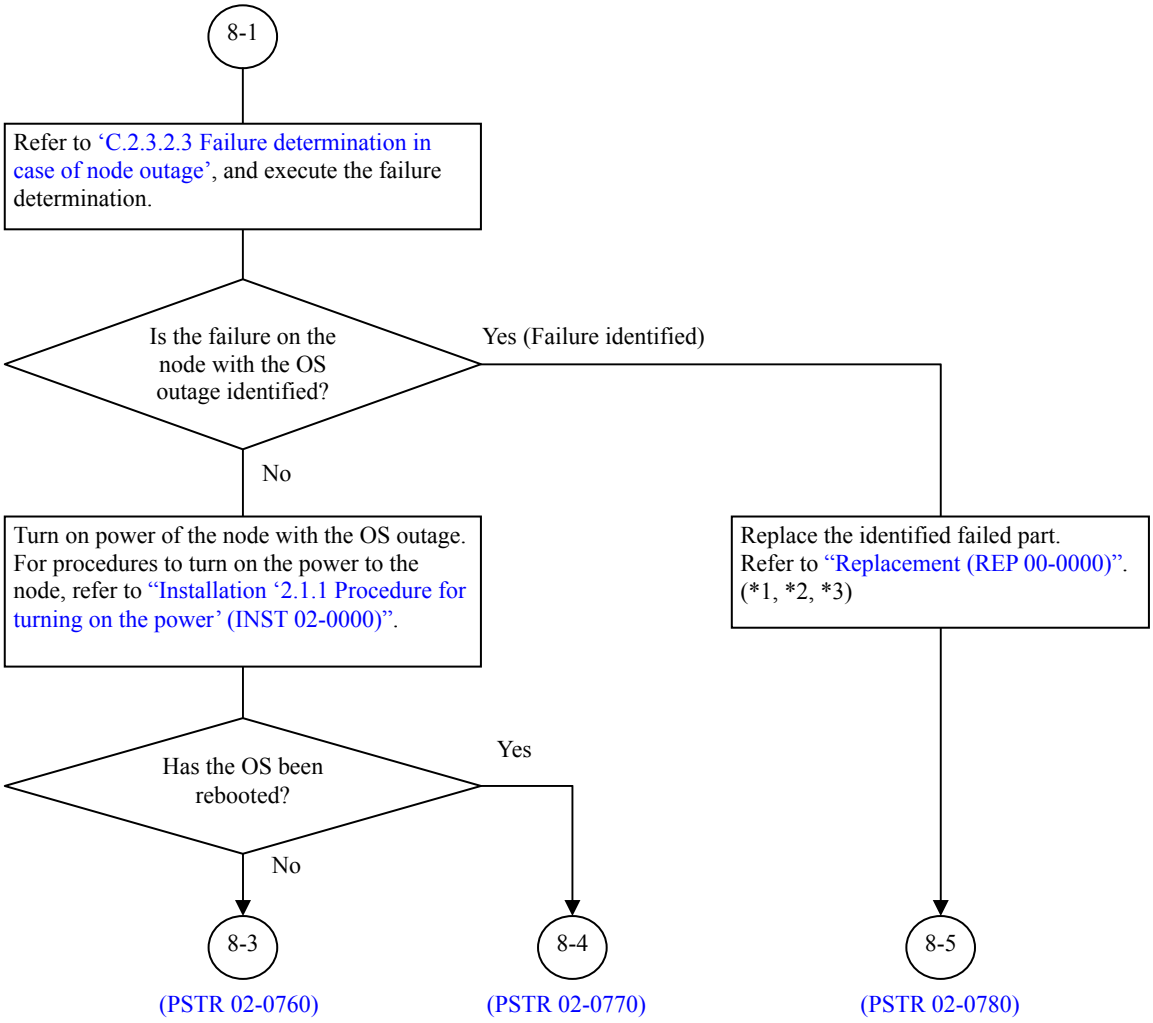
*1: Report to the system administrator that the operation is stopped completely during the replacement of the management port.

*2: Replace the parts and confirm after the replacement with the heartbeat cable and the management port cable removed. Do not request the system administrator to execute failback.

*3: Refer to "Replacement '1.6 Replacing the Management LAN IP-SW (IP Switch) (1) Replacement procedure while the node is in operation' (REP 01-0290)".
If it is the management LAN IP-SW owned by the customer, request the customer to replace the management LAN IP-SW. The maintenance personnel should execute the rest of the operation after the report that the replacement is completed.

Figure C.2.3.2.2-8 Flow of Management Network Failure Determination (2/6)

Copyright © 2011, 2015, Hitachi, Ltd.



*1: There is a node that needs to be replaced the parts at the support center. In this case, explain to the customer that the operation must be done by just one side node. The recovery operation from here executes some other day when the node is returned and verified that it works normally. Therefore, stop the maintenance operation here in the meanwhile.

*2: Replace the parts and confirm after the replacement with the heartbeat cable and the management port cable removed. Do not request the system administrator to execute failback.

*3: Make sure to collect Simple log by using HATP before the parts replacement.

Figure C.2.3.2.2-8 Flow of Management Network Failure Determination (3/6)

Copyright © 2011, 2015, Hitachi, Ltd.

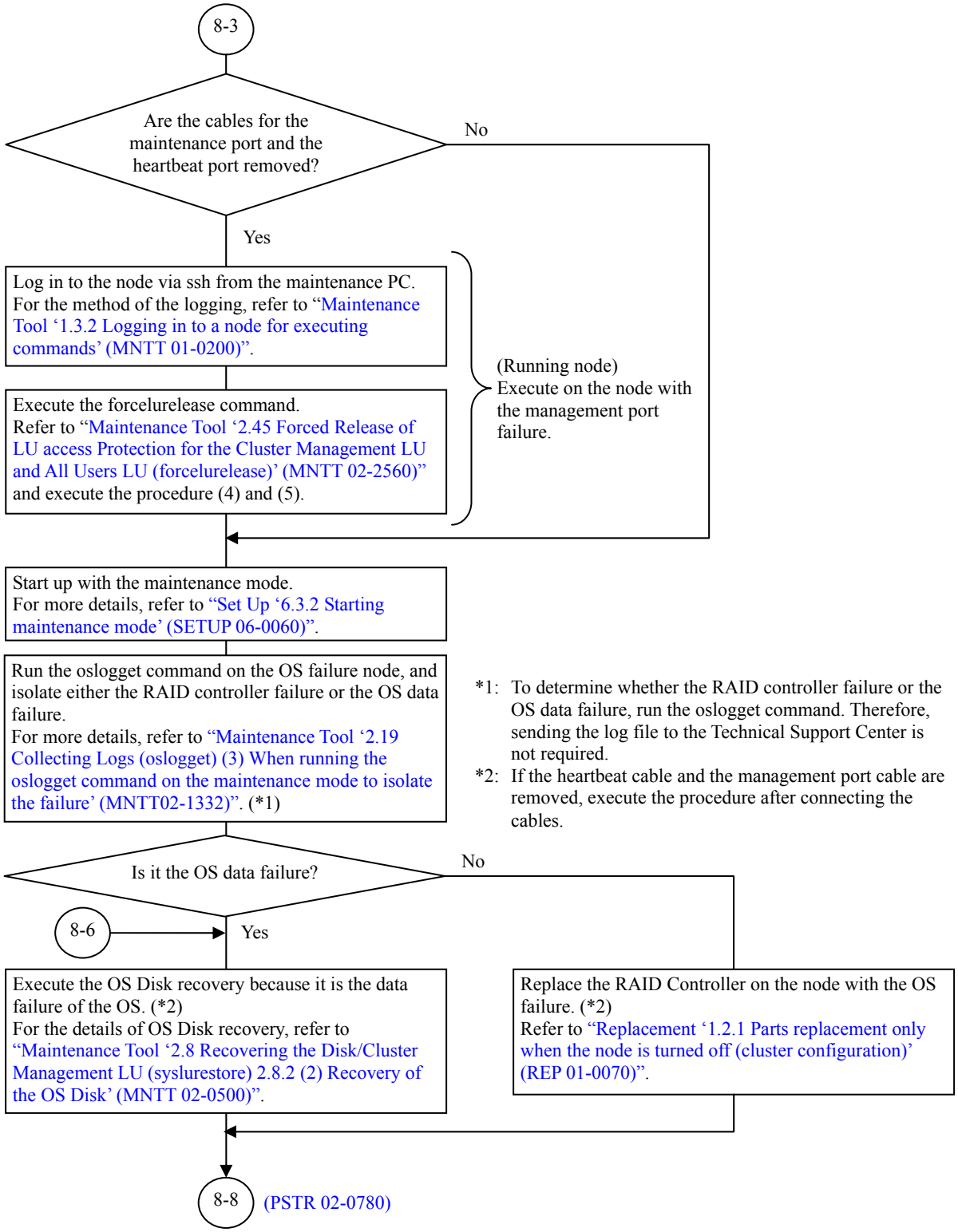
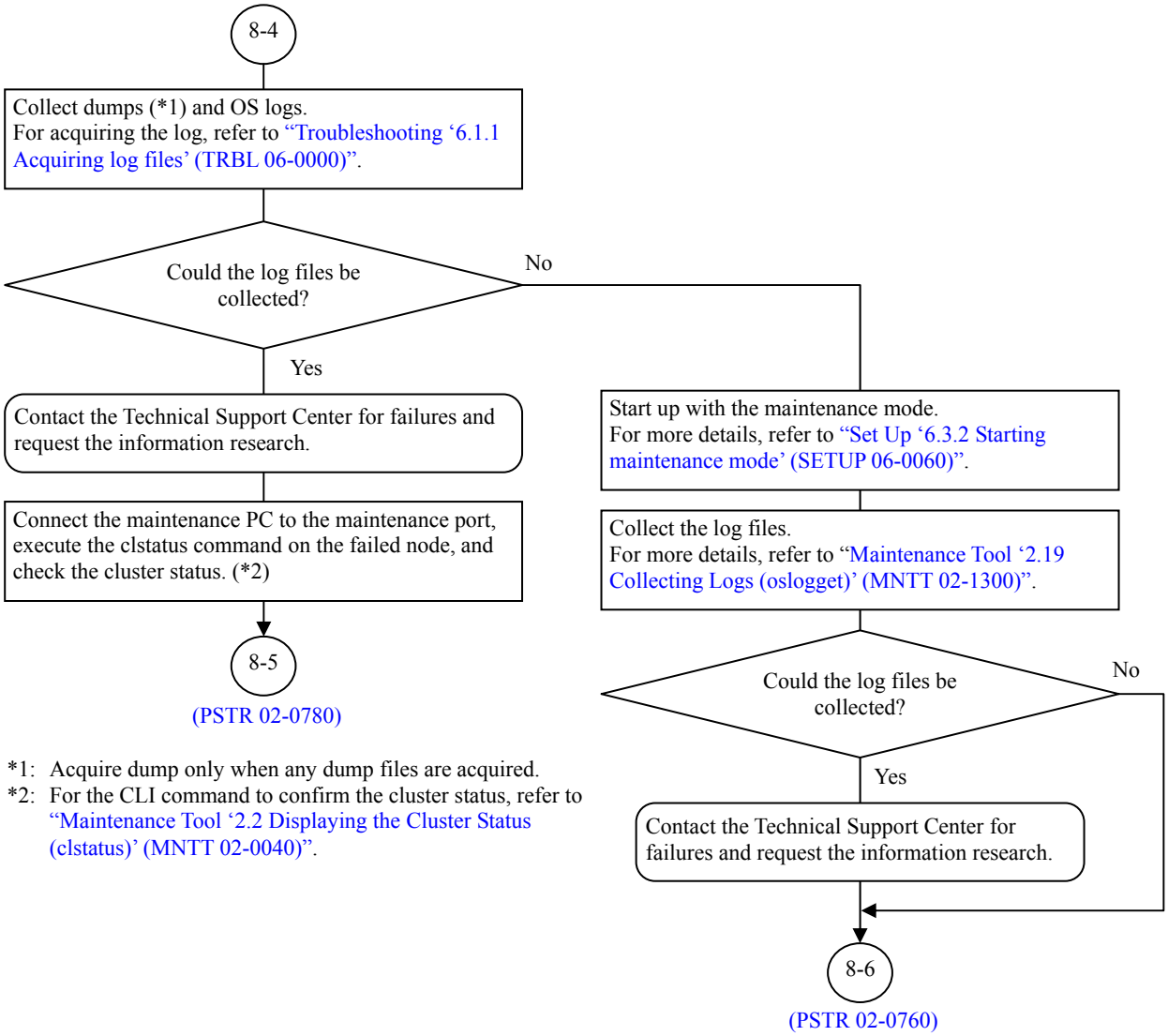


Figure C.2.3.2.2-8 Flow of Management Network Failure Determination (4/6)

Copyright © 2011, 2015, Hitachi, Ltd.



*1: Acquire dump only when any dump files are acquired.
*2: For the CLI command to confirm the cluster status, refer to "Maintenance Tool '2.2 Displaying the Cluster Status (clstatus)' (MNTT 02-0040)".

Figure C.2.3.2.2-8 Flow of Management Network Failure Determination (5/6)

Copyright © 2011, 2015, Hitachi, Ltd.

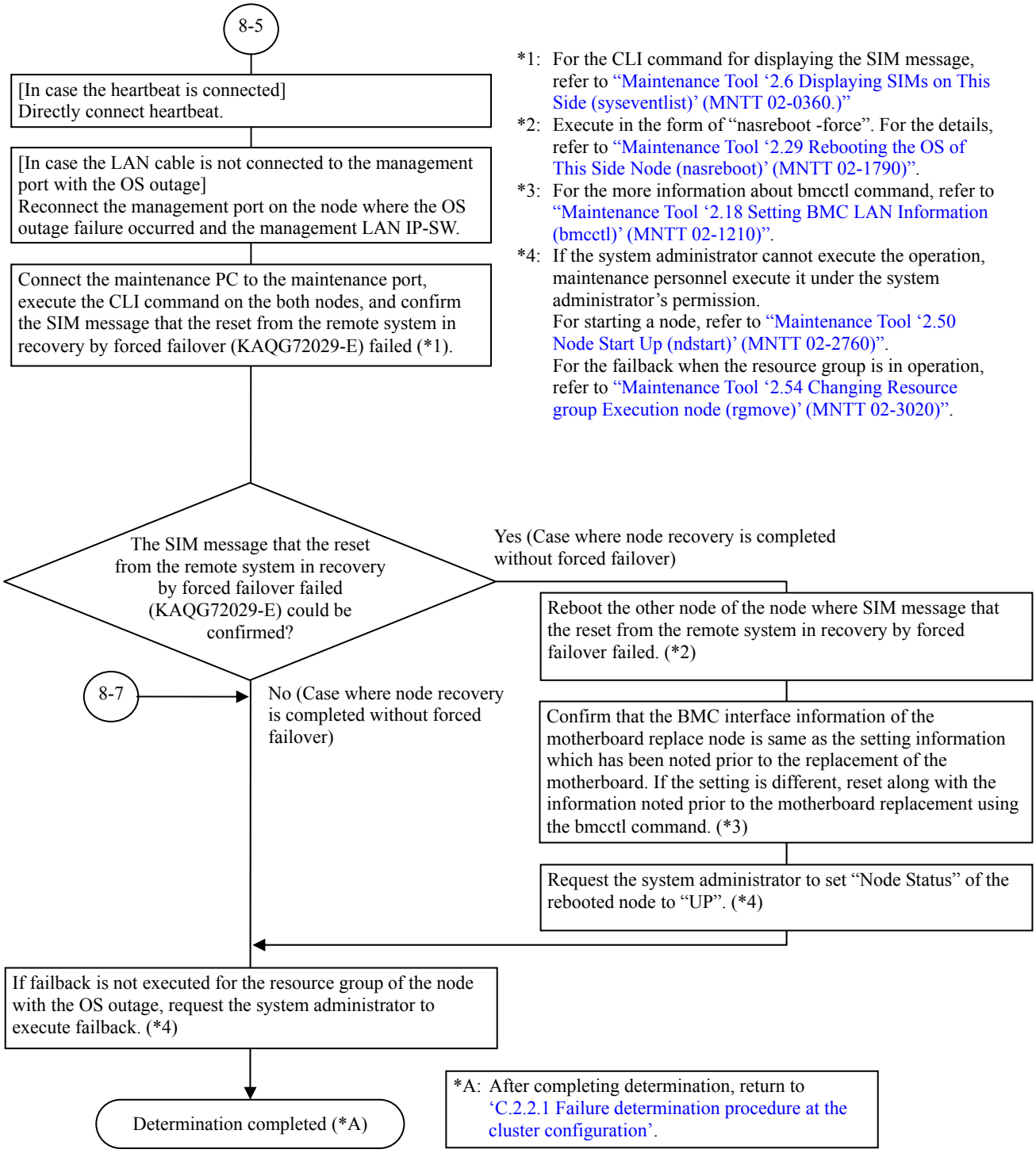
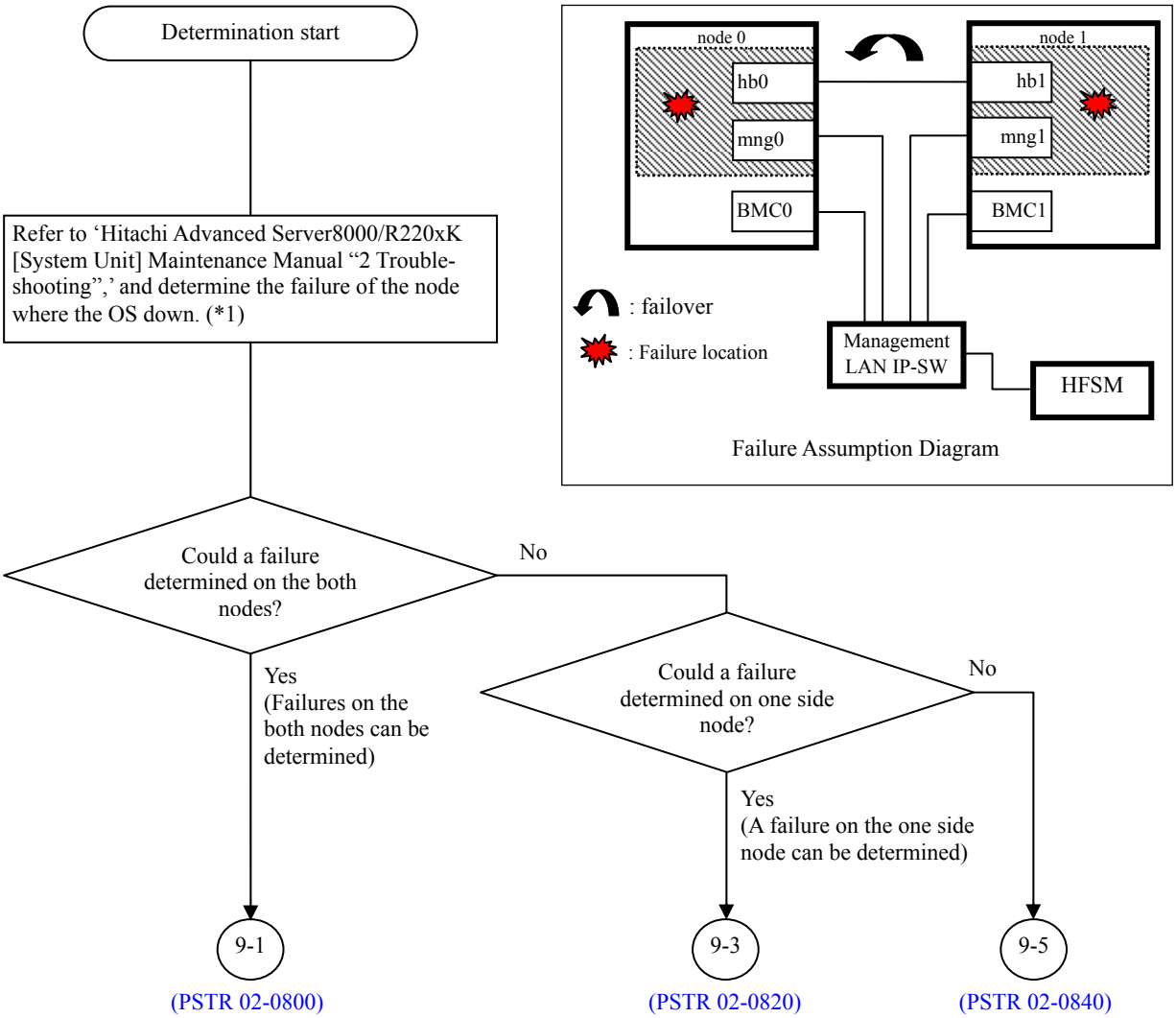


Figure C.2.3.2.2-8 Flow of Management Network Failure Determination (6/6)

Copyright © 2011, 2015, Hitachi, Ltd.

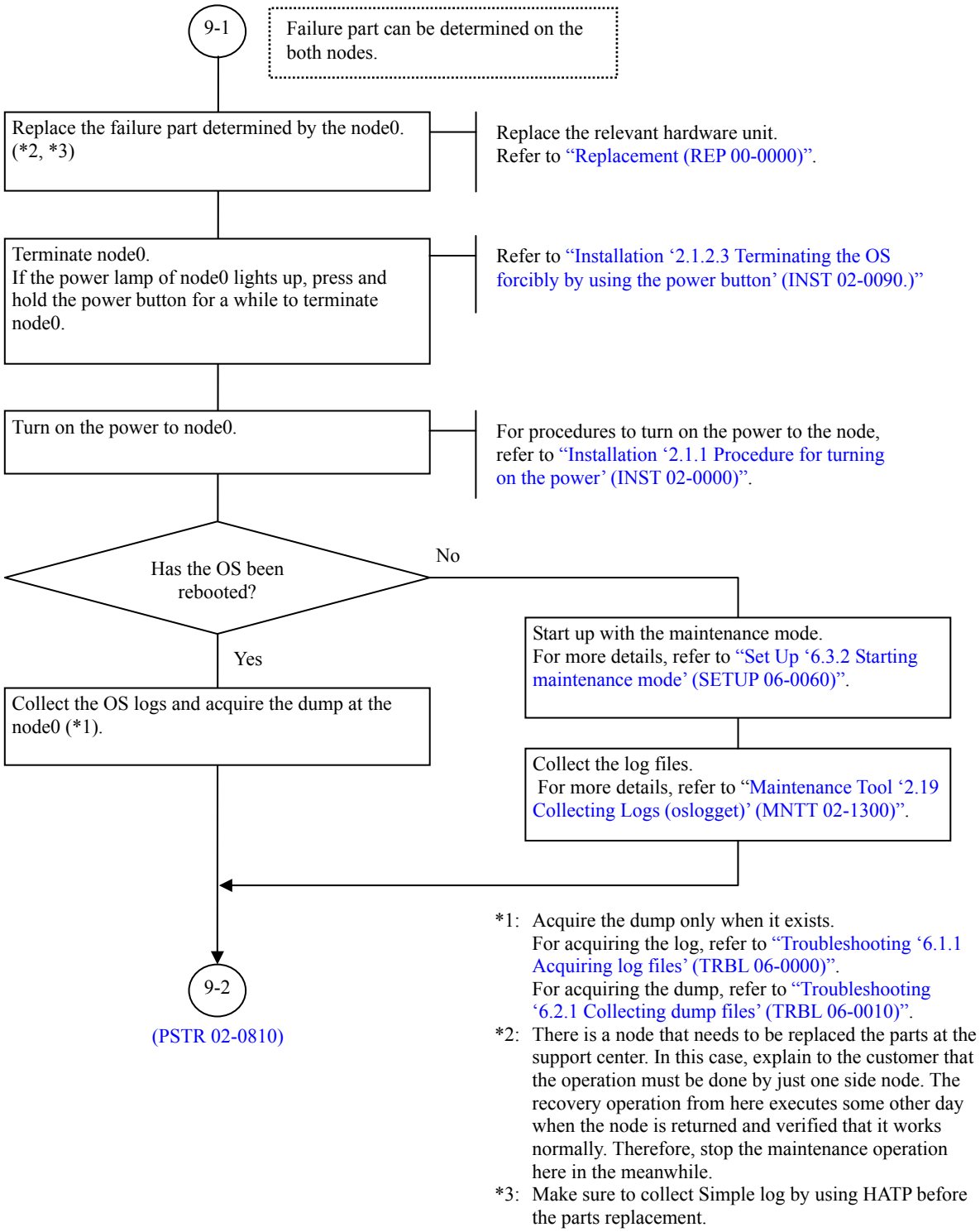
(9) Dual failure of OS



*1: Determining a candidate failure part means that the RC can be determined from the result of HATP, or a failure candidate can be determined from the MAINTENANCE lamp display.
However, when the MAINTENANCE lamp lights up as "01" and it is not dual failure of the embedded HDD, or when there is no problem on the result of the HATP, a failure in the hardware such as on RAID controller might not be detected. In this case, assume that the hardware failure cannot be determined.

Figure C.2.3.2.2-9 Flow of Management Network Failure Determination (1/6)

Copyright © 2011, 2013, Hitachi, Ltd.



*1: Acquire the dump only when it exists.
For acquiring the log, refer to "Troubleshooting '6.1.1 Acquiring log files' (TRBL 06-0000)".
For acquiring the dump, refer to "Troubleshooting '6.2.1 Collecting dump files' (TRBL 06-0010)".

*2: There is a node that needs to be replaced the parts at the support center. In this case, explain to the customer that the operation must be done by just one side node. The recovery operation from here executes some other day when the node is returned and verified that it works normally. Therefore, stop the maintenance operation here in the meanwhile.

*3: Make sure to collect Simple log by using HATP before the parts replacement.

Figure C.2.3.2.2-9 Flow of Management Network Failure Determination (2/6)

Copyright © 2011, 2013, Hitachi, Ltd.

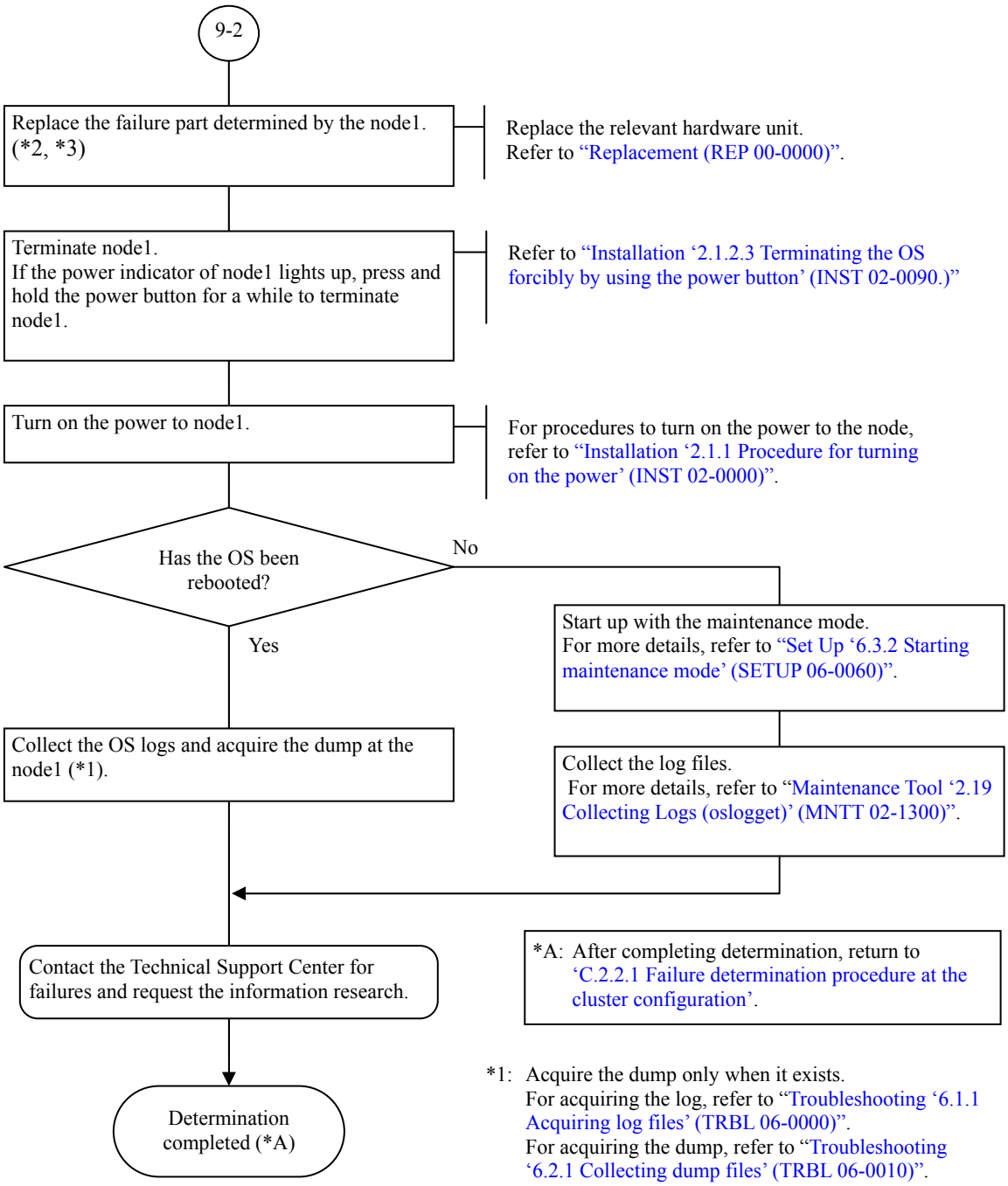
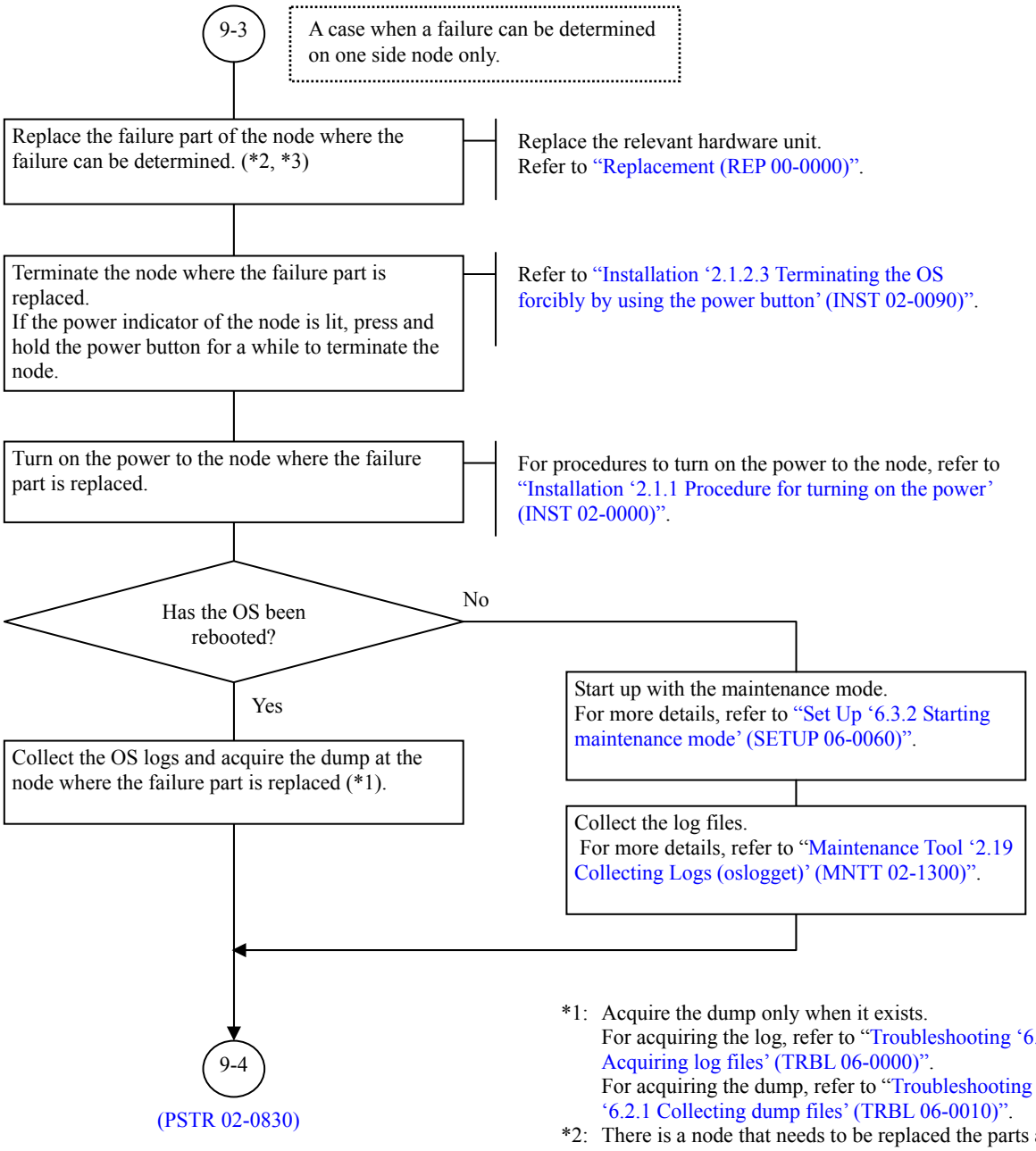


Figure C.2.3.2.2-9 Flow of Management Network Failure Determination (3/6)

Copyright © 2011, 2013, Hitachi, Ltd.



*1: Acquire the dump only when it exists.
For acquiring the log, refer to "Troubleshooting '6.1.1 Acquiring log files' (TRBL 06-0000)".
For acquiring the dump, refer to "Troubleshooting '6.2.1 Collecting dump files' (TRBL 06-0010)".

*2: There is a node that needs to be replaced the parts at the support center. In this case, explain to the customer that the operation must be done by just one side node. The recovery operation from here executes some other day when the node is returned and verified that it works normally. Therefore, stop the maintenance operation here in the meanwhile.

*3: Make sure to collect Simple log by using HATP before the parts replacement.

Figure C.2.3.2.2-9 Flow of Management Network Failure Determination (4/6)

Copyright © 2011, 2013, Hitachi, Ltd.

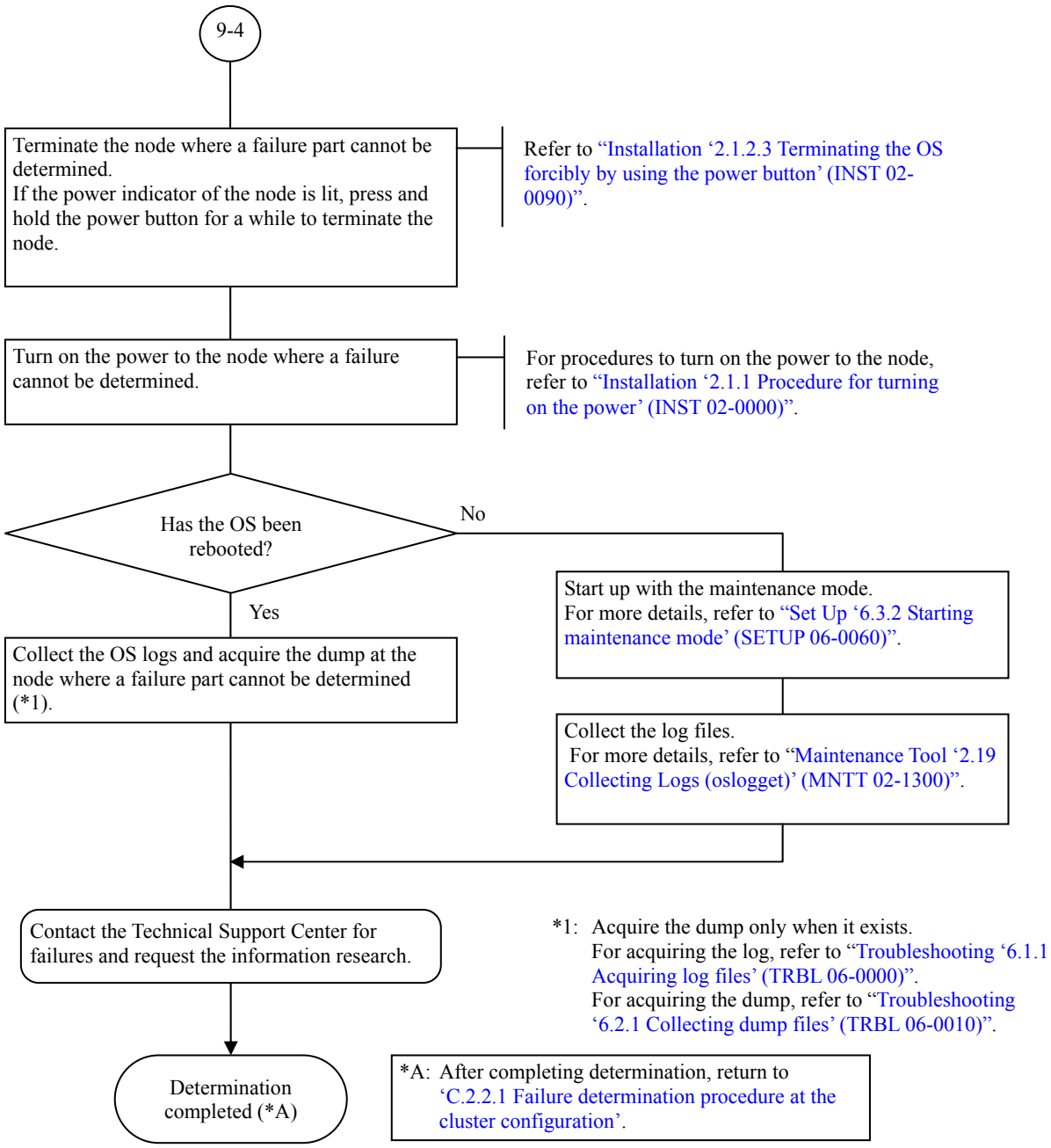


Figure C.2.3.2.2-9 Flow of Management Network Failure Determination (5/6)

Copyright © 2011, 2013, Hitachi, Ltd.

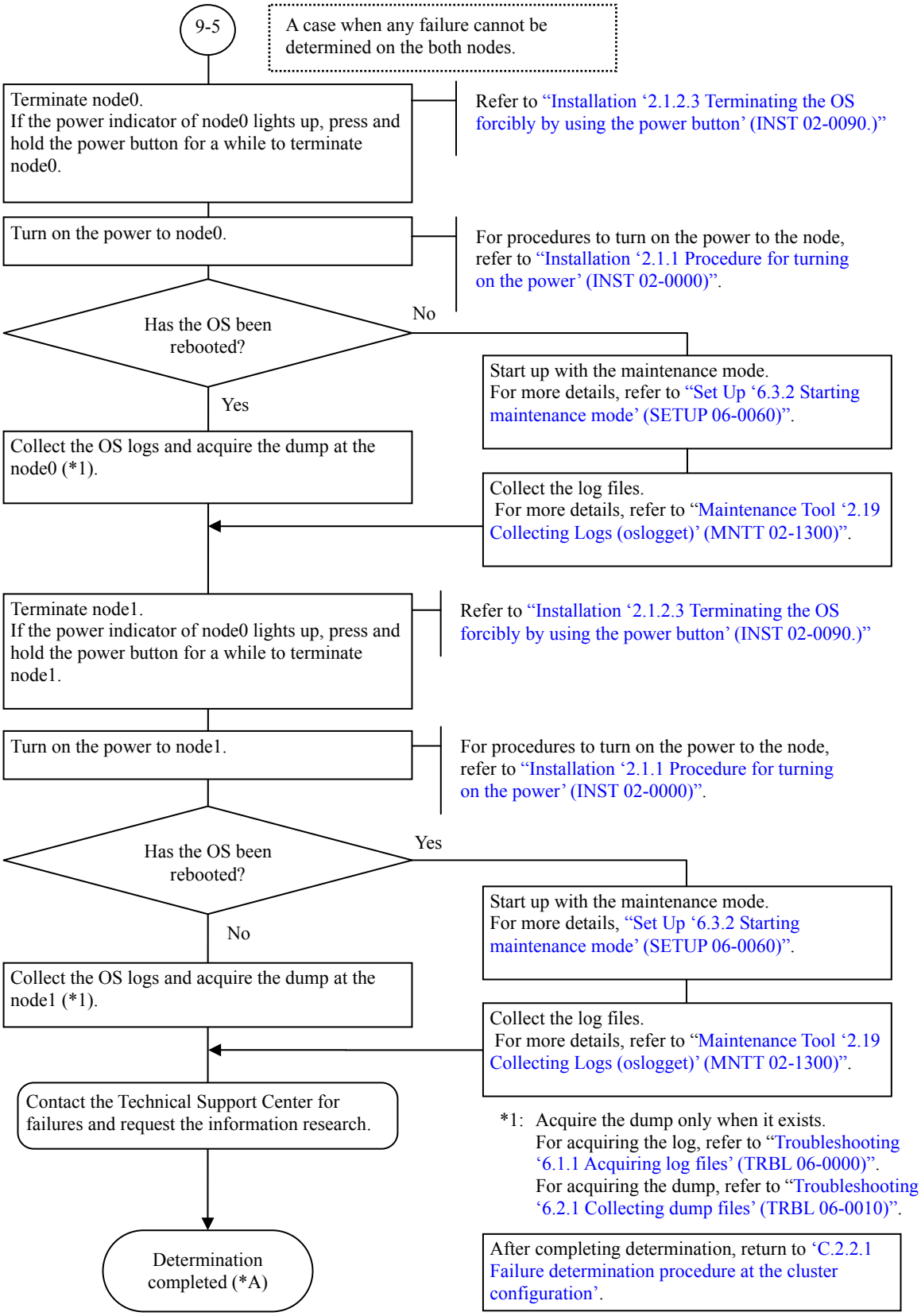
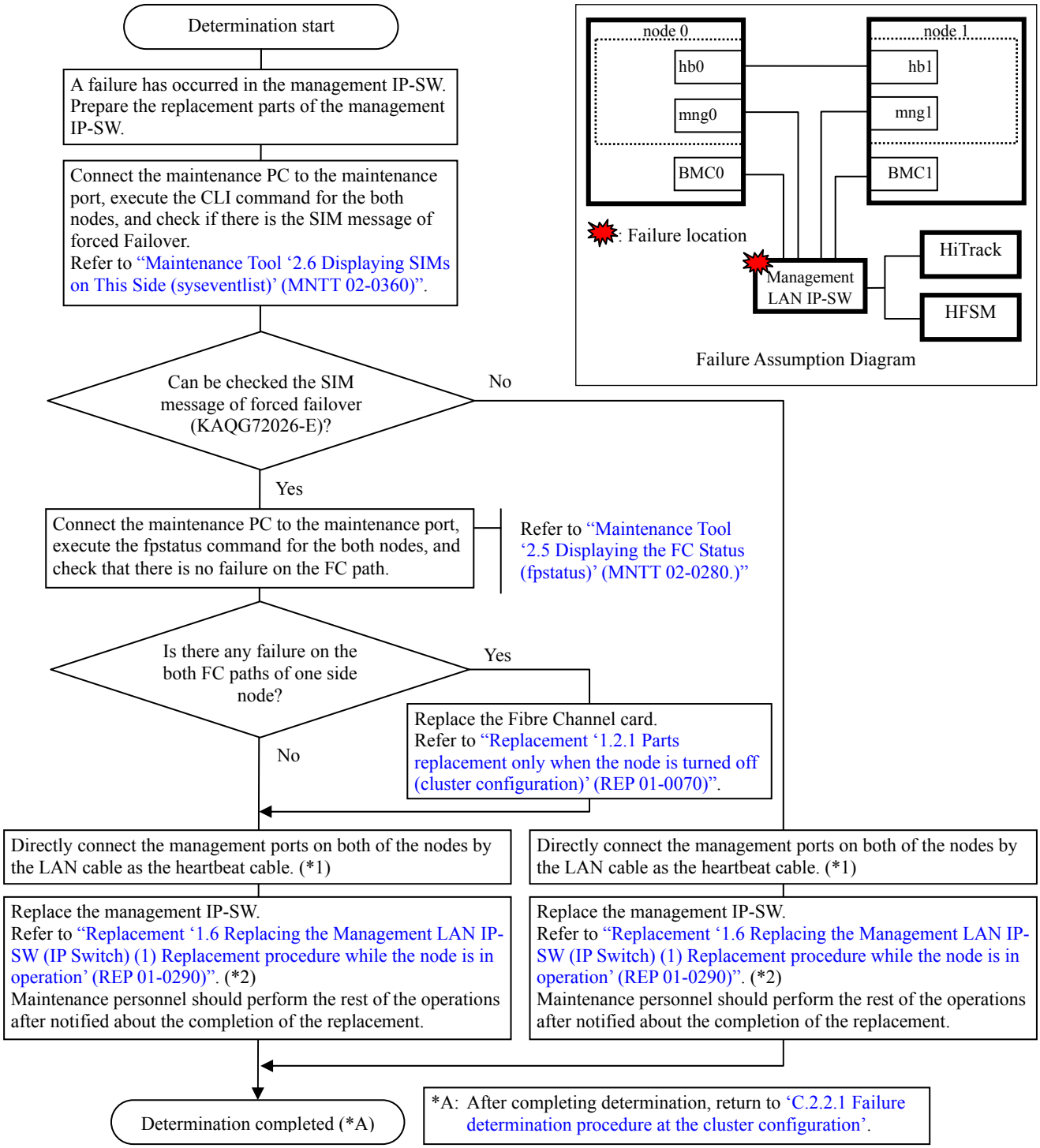


Figure C.2.3.2.2-9 Flow of Management Network Failure Determination (6/6)

Copyright © 2011, 2013, Hitachi, Ltd.

(10) Failure in the management IP-SW



*1: Remove the LAN cable connecting between the management port on the node 0 and the management LAN IP-SW from the management LAN IP-SW, and then connect to the management port on the node 1.

*2: Before executing the procedure (1-3) (c) that is described in the "Replacement '1.6 Replacing the Management LAN IP-SW (IP Switch) (1) Replacement procedure while the node is in operation' (REP 01-0290)", the other side node of the node where the SIM message of forced failover is confirmed is reset. After confirming the startup of the other side node, execute the procedure (1-3) (c) and later.

Figure C.2.3.2.2-10 Flow of Management Network Failure Determination

Copyright © 2011, 2015, Hitachi, Ltd.

C.2.3.2.3 Failure determination in case of node outage

Refer to “Hitachi Advanced Server8000/RS220xK [System Unit] Maintenance Manual ‘2.Trouble-shooting’,” and determine a failure on the node in which the OS down, and then return to the procedure described in ‘C.2.3.2.2 Flow of management network failure determination’ to continue the determination operation.

Determining a candidate failure part means that the RC can be determined from the result of HATP, or a failure candidate can be determined from the MAINTENANCE lamp display.

However, when the MAINTENANCE lamp lights up as “01” and it is not dual failure of the embedded HDD, or when there is no problem on the result of the HATP, a failure in the hardware such as on RAID controller might not be detected. In this case, assume that the hardware failure cannot be determined.

Copyright © 2011, 2013, Hitachi, Ltd.

C.2.3.3 Determining the node failure when no failover occurs

The failure determination and the failed part when SIM of failover is not displayed are described below.

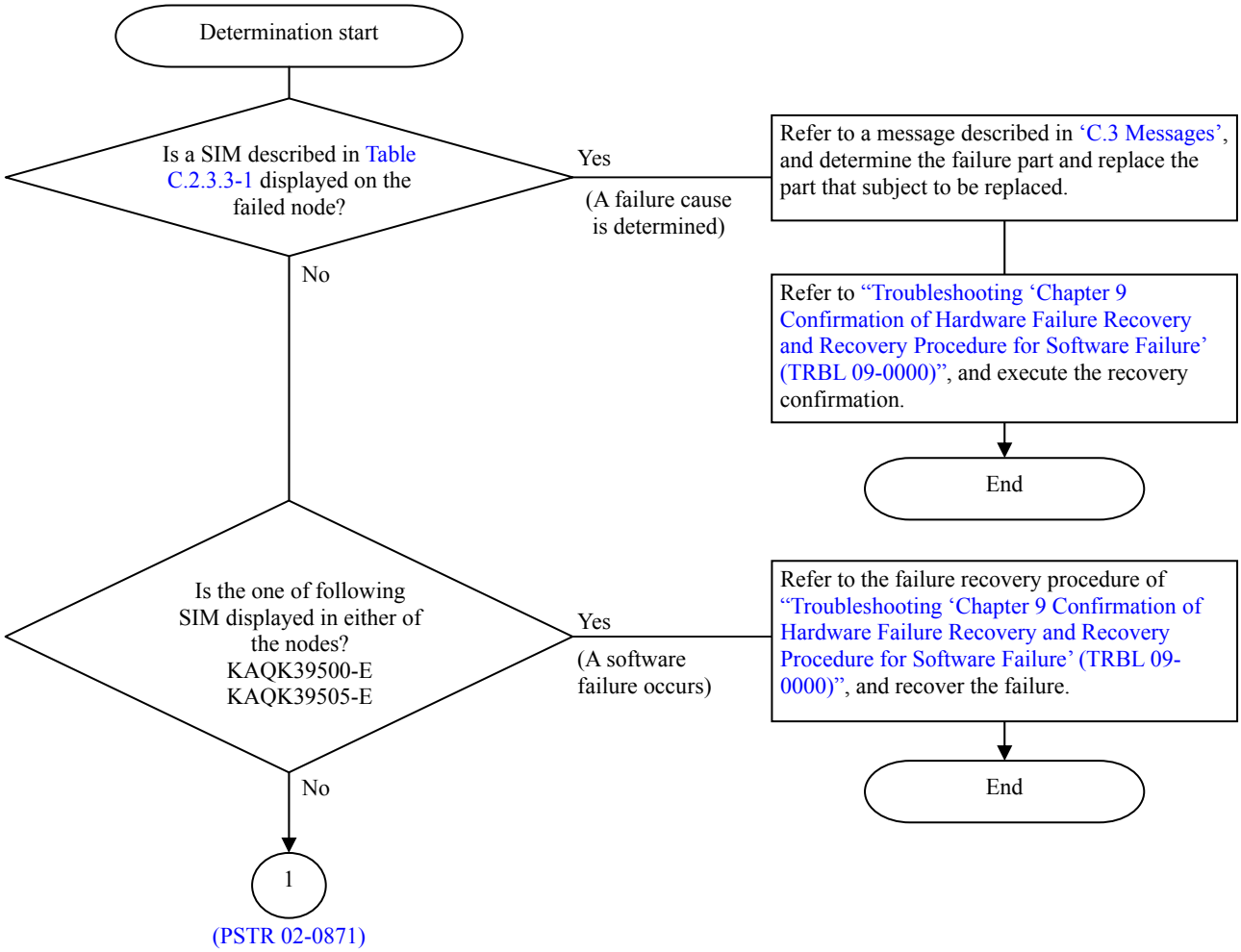


Figure C.2.3.3-1 Determining the node failure when failover has not occurred (1/2)

Copyright © 2011, 2013, Hitachi, Ltd.

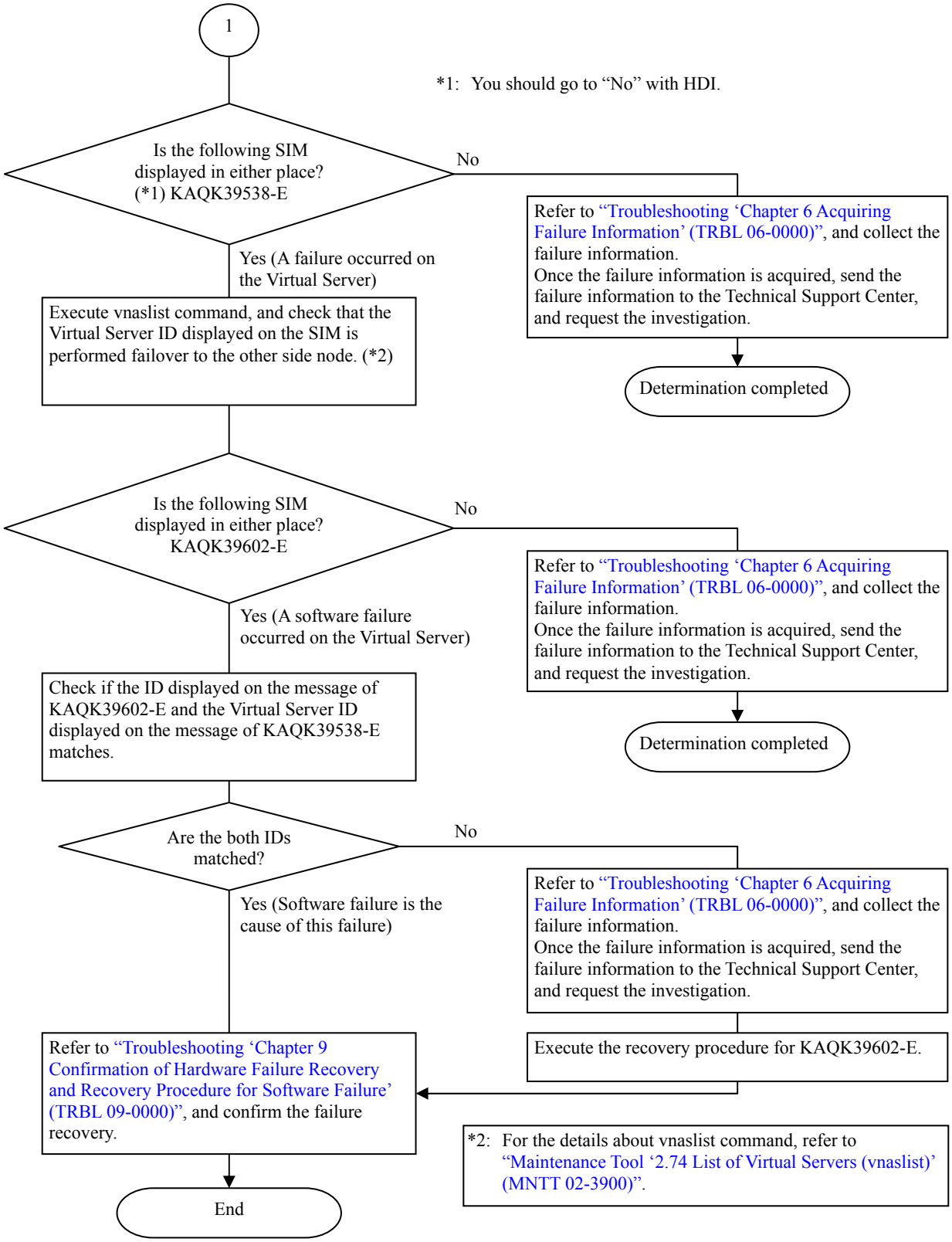


Figure C.2.3.3-1 Determining the node failure when failover has not occurred (2/2)

Copyright © 2011, 2014, Hitachi, Ltd.

Table C.2.3.3-1 Failed parts shown by SIM

#	SIM	Lamp status	Checking the status by the hwstatus command (*1)	Failed part
1	KAQG72012-W	—	Is the Heartbeat LAN port status “Link down”?	Heartbeat LAN port or Heartbeat LAN cable (*2) (*3)
2	KAQG81003-W	—	Is the port status “Link down”?	Extension NIC port or cable (*2)
3	KAQK30801-E	—	—	Determine a failure part from the RC described in SIM and the continuous log (*4)
4	KAQK39504-E	—	Is the status of all ports of NIC “Link down”?	—
5	KAQK39527-E	—	—	Pool exhaustion (*5)

*1: For the hwstatus command, refer to ‘B.3.1 Displaying the Hardware Status (hwstatus)’.
*2: When it is not recovered even if the cable is replaced, it is a port failure.
*3: In case of a port failure, ping from the management PC or maintenance PC, and specify which of the nodes has the port failure.
*4: For the determination from the RC and the continuous log, refer to “Hitachi Advanced Server 8000/RS220xK [System Unit] Maintenance Manual”.
*5: Ask the system administrator to recover the pool exhaustion.

Copyright © 2011, 2013, Hitachi, Ltd.

C.2.3.4 Determining the node failure when failover occurred

The failure determination and the failed part when SIM of failover is displayed are described.

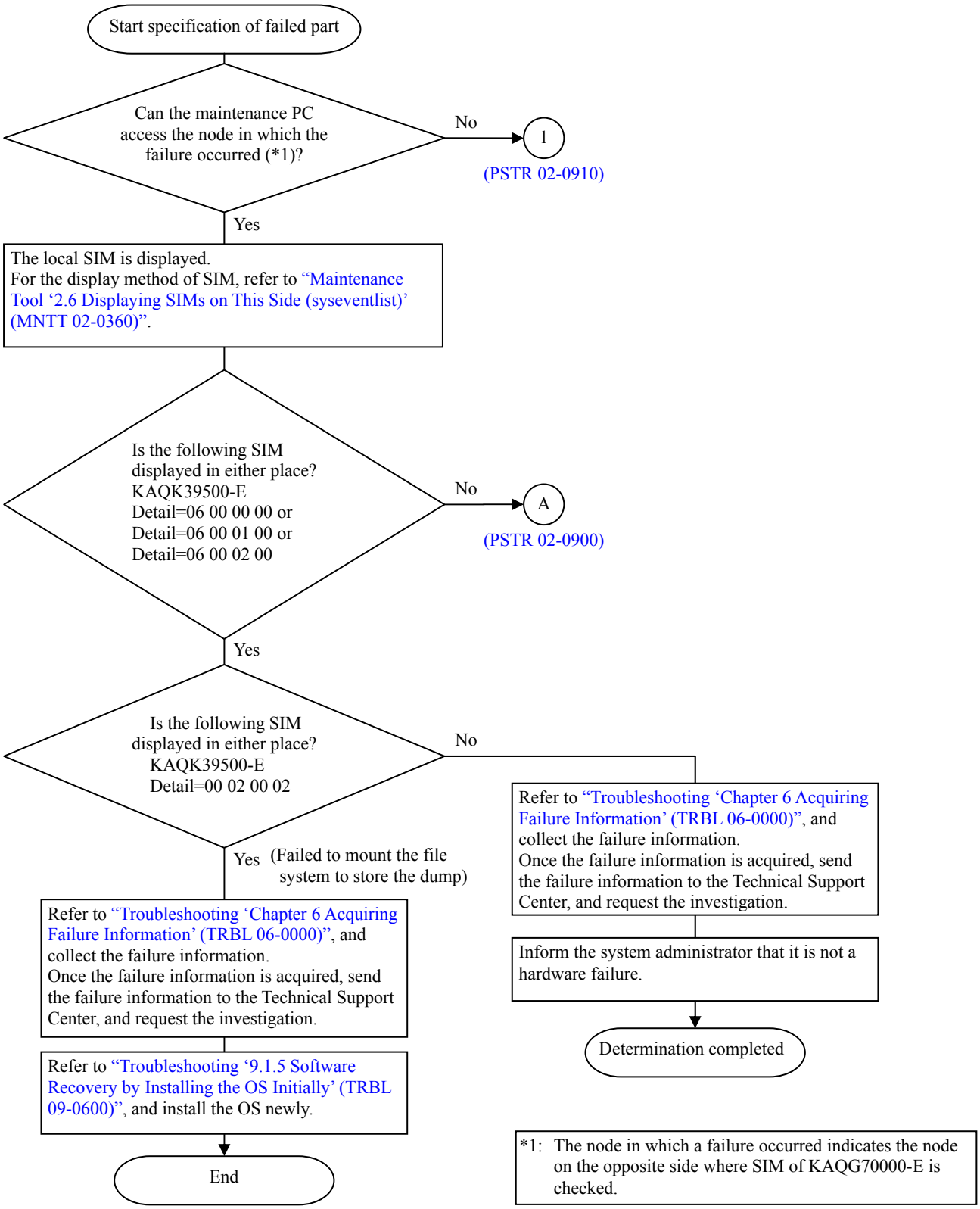


Figure C.2.3.4-1 Determining the node failure when failover occurred (1/7)

Copyright © 2011, 2014, Hitachi, Ltd.

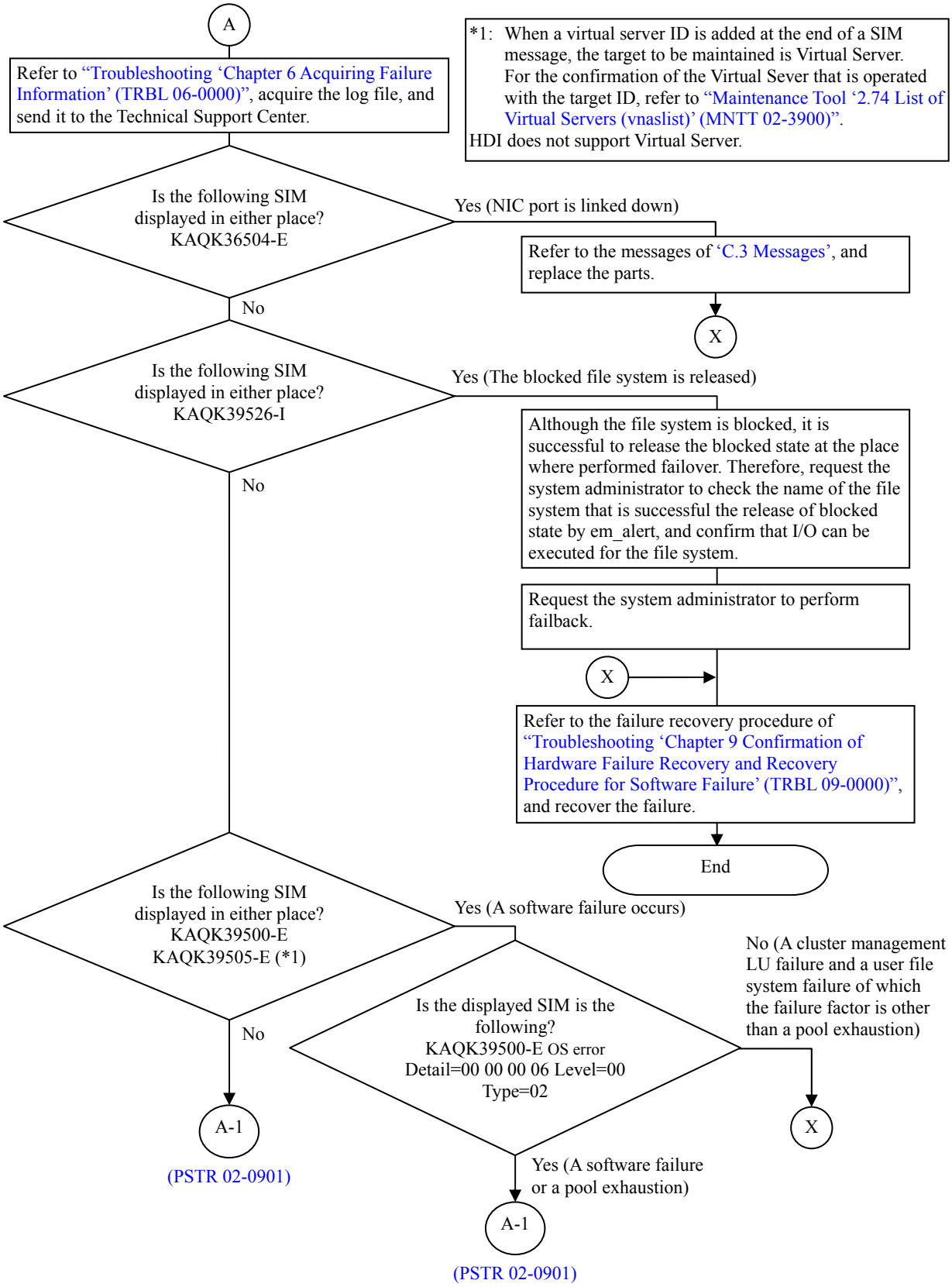


Figure C.2.3.4-1 Determining the node failure when failover occurred (2/7)

Copyright © 2011, 2013, Hitachi, Ltd.

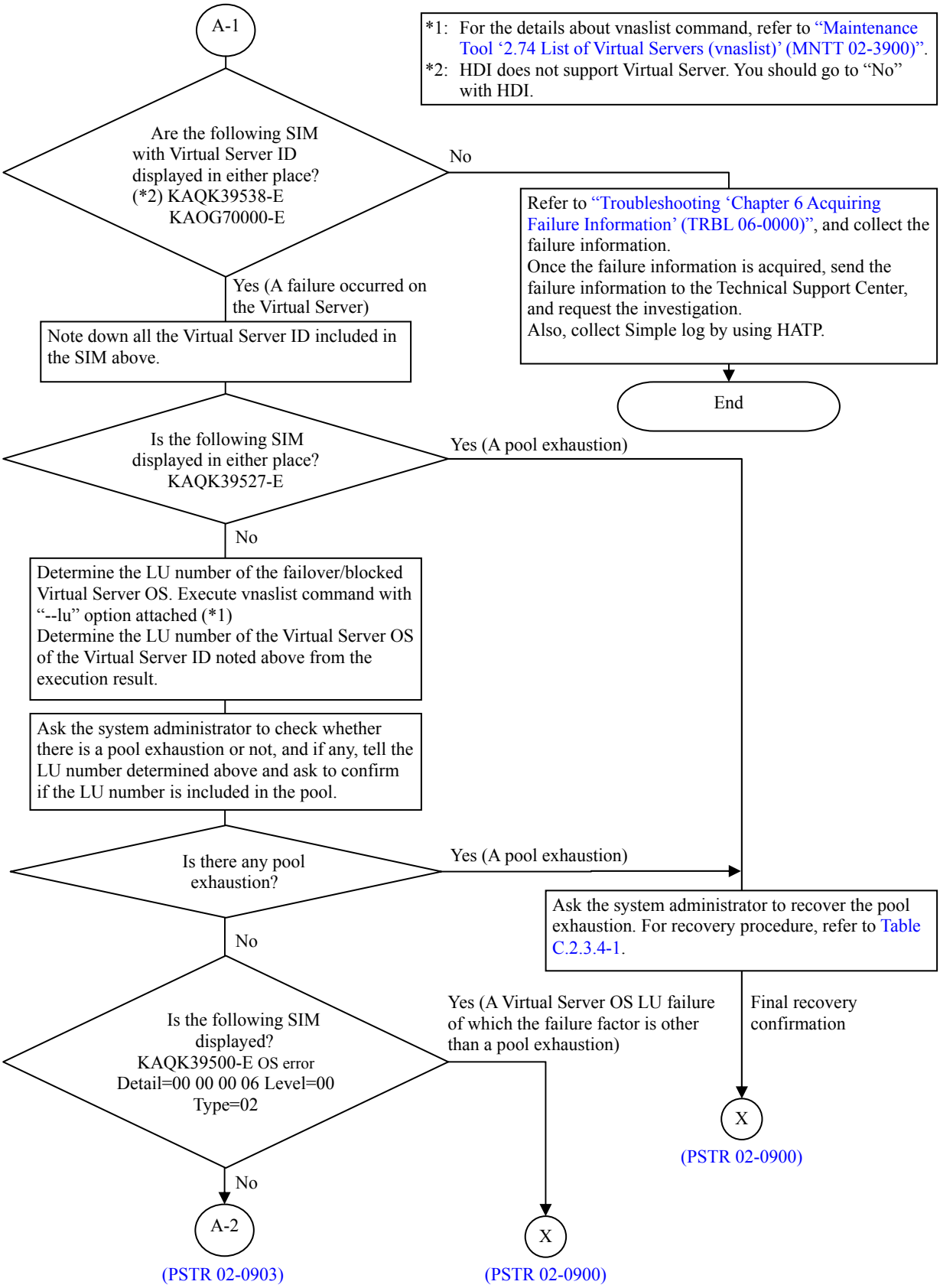


Figure C.2.3.4-1 Determining the node failure when failover has not occurred (3/7)

Copyright © 2011, 2014, Hitachi, Ltd.

Table C.2.3.4-1 Recovery procedures for a failure due to a pool exhaustion

#	Procedure	Operator
1	Ask an expansion of the pool etc. to solve the pool exhaustion. Proceed to #2 if expansion is already done.	System administrator
2	Ask to confirm that if there is any LU that is used as Virtual Server OS LU, “all capacity allocation mode” or “full allocation” is not enabled in the pool which expanded the capacity in #1.	
3	Ask to restart all the Virtual Servers that belong to the pool which capacity is not sufficient. Make sure to tell that restart is not necessary for the Virtual Server of which the Virtual Server OS is also blocked or the Virtual Server which meets the definition of #2. Proceed to #4 if restart is already done.	
4	In the case the Virtual Server OS is also blocked or the condition meets #2, perform #5. If not, perform #6.	
5	Ask to recover the Virtual Server OS LU. For the reference place in User’s Guide, refer to “General ‘Reference Place in User's Guide for Operating Procedures Table 4 ‘Recovering a virtual server OS LU’’ (GENE 00-0050)”. Proceed to #6 if recovery is already done.	
6	If the target disk array subsystem is the AMS2000 series or the HUS100 series, ask to enable “all capacity allocation mode” for all the Virtual Server OS LU. Proceed to #7 if it is already enabled. If the target disk array subsystem is VSP Gx00/VSP Fx00, or VSP G1000 whose DKCMAIN version is 08-02-2x or later, ask the system administrator to set the “full allocation” to [enable] for all Virtual Server OS LUs.	
7	Return to Figure C.2.3.4-1 and execute the rest of the flow.	

Copyright © 2012, 2016, Hitachi, Ltd.

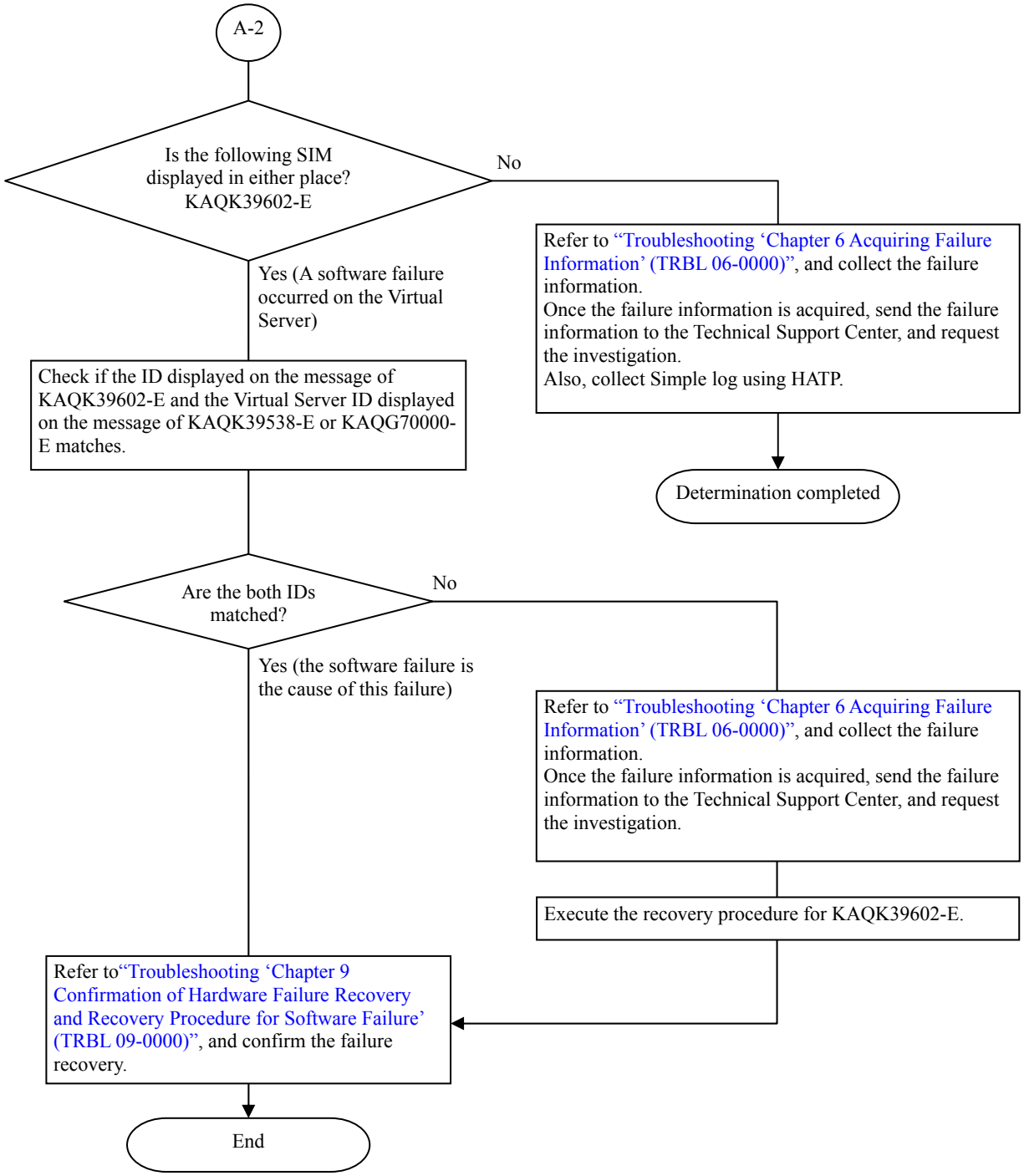
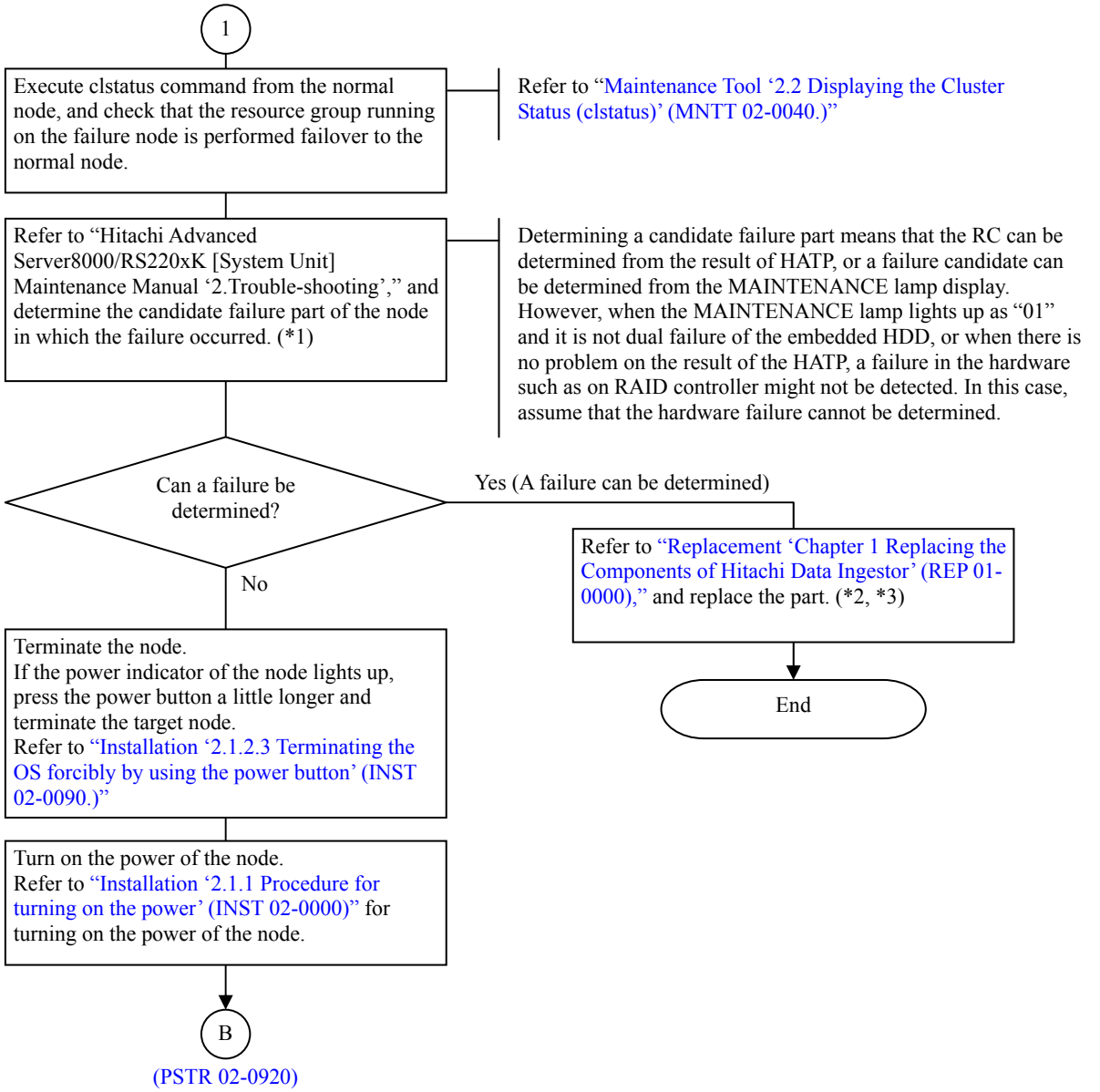


Figure C.2.3.4-1 Determining the node failure when failover occurred (4/7)

Copyright © 2012, 2013, Hitachi, Ltd.



*1: There is no problem to reboot the failed node for executing HATP.
*2: There is a node that needs to be replaced the parts at the support center. In this case, explain to the customer that the operation must be done by just one side node. The recovery operation from here executes some other day when the node is returned and verified that it works normally. Therefore, stop the maintenance operation here in the meanwhile.
*3: Make sure to collect Simple log by using HATP before the parts replacement.

Figure C.2.3.4-1 Determining the node failure when failover occurred (5/7)

Copyright © 2011, 2013, Hitachi, Ltd.

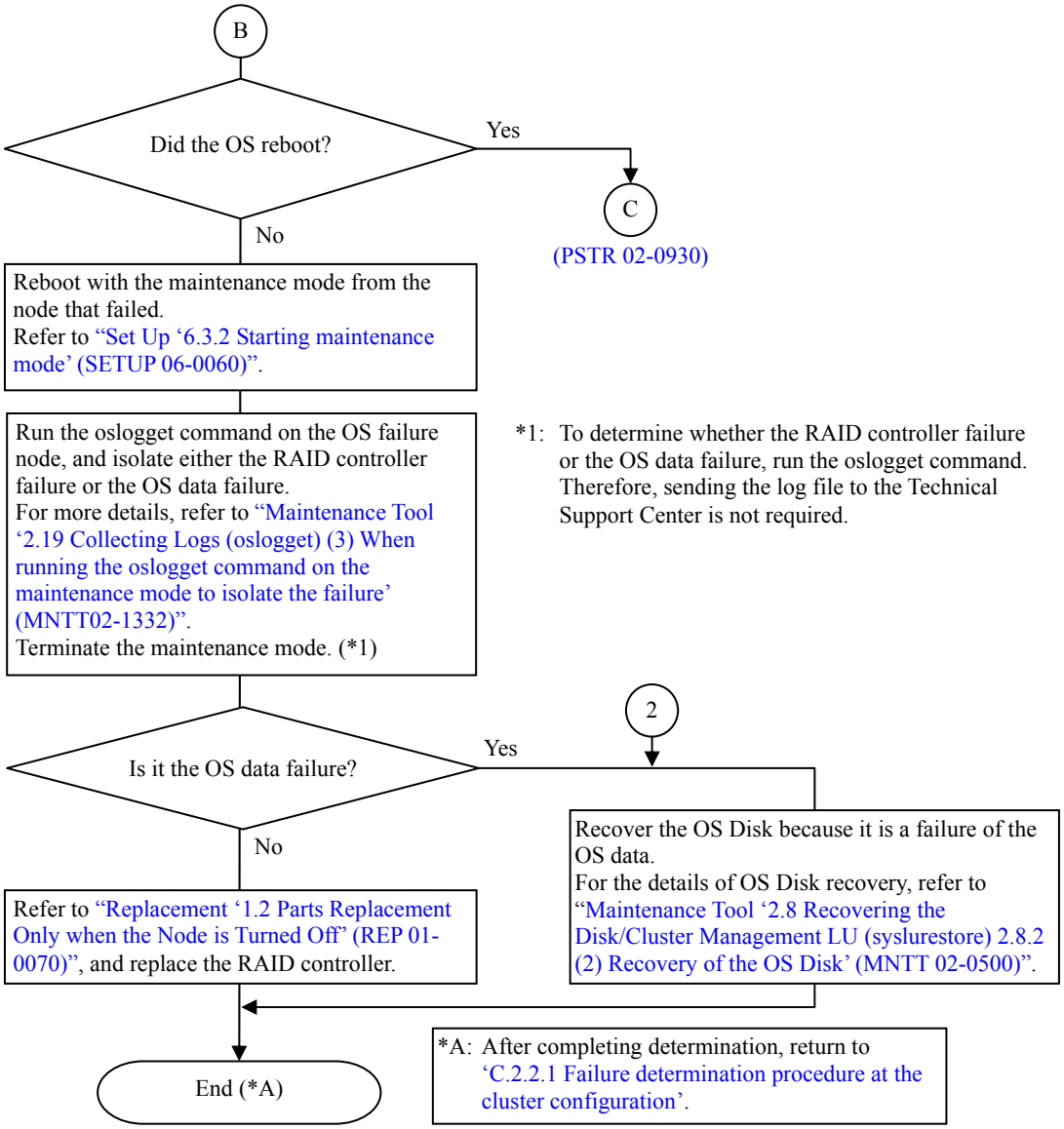


Figure C.2.3.4-1 Determining the node failure when failover occurred (6/7)

Copyright © 2011, 2015, Hitachi, Ltd.

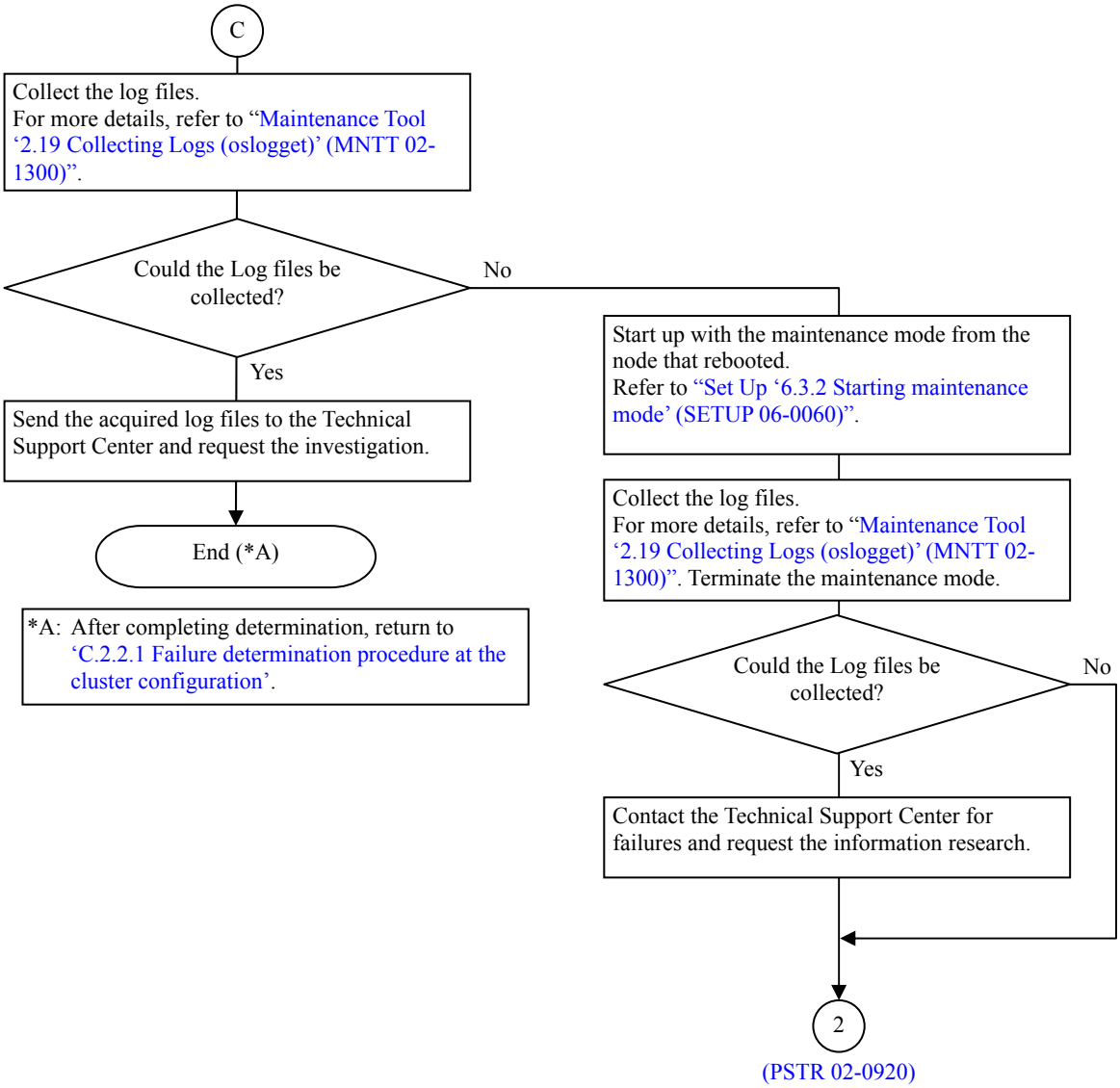


Figure C.2.3.4-1 Determining the node failure when failover occurred (7/7)

Copyright © 2011, 2013, Hitachi, Ltd.

C.2.3.5 Determination of node failure in the single node configuration

The following explains the failure determination and the failure part in the single node configuration.

Table C.2.3.5-1 Table of Determination matrix of the node operating status

Ping for the BMC port (*1)	OS starts up confirmation (*2)	ssh login for the maintenance port (*3)	Result of the determination
Y	Y	Y	node in operation
		N	node in operation (Maintenance port failure)
	N	—	node down
N	—	Y	node in operation (BMC failure)
		N	Ask the system administrator if the data can be accessed.

*1: Connect directly the BMC port to the maintenance PC with a LAN cable, and execute ping command for the BMC port.

*2: Check if the OS starts from the remote console of BMC. For the details, refer to "Set Up '1.4 Connection Confirmation of the Remote Console' (SETUP 01-0010)".

*3: Connect directly the maintenance port to the maintenance PC with a LAN cable, and check if the ssh login can be done. For the details, refer to "Maintenance Tool '1.3 Procedures for Operating Commands' (MNTT 01-0200)".

Copyright © 2011, 2013, Hitachi, Ltd.

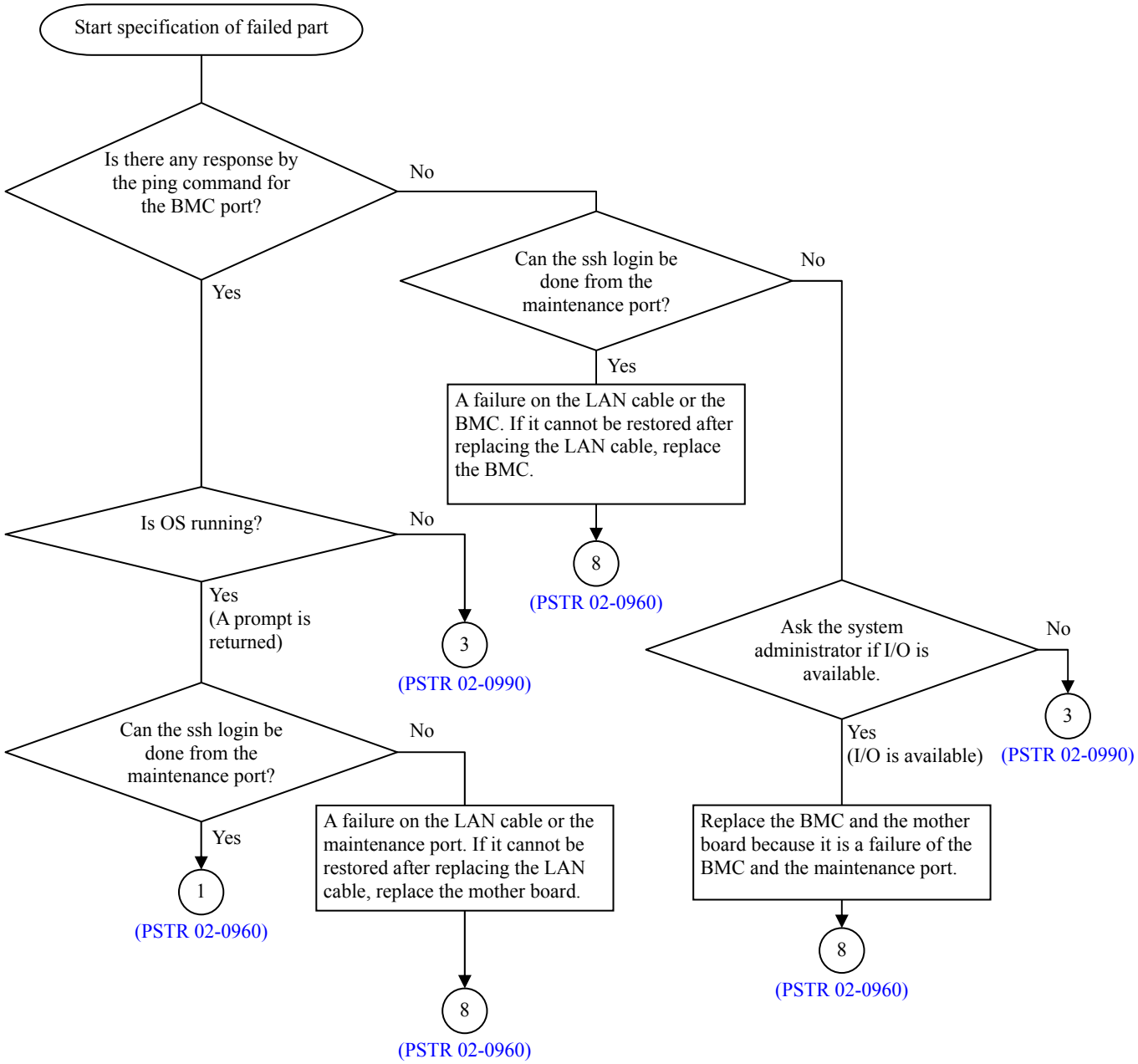


Figure C.2.3.5-1 Determining the node failure in the single node configuration (1/8)

Copyright © 2011, 2013, Hitachi, Ltd.

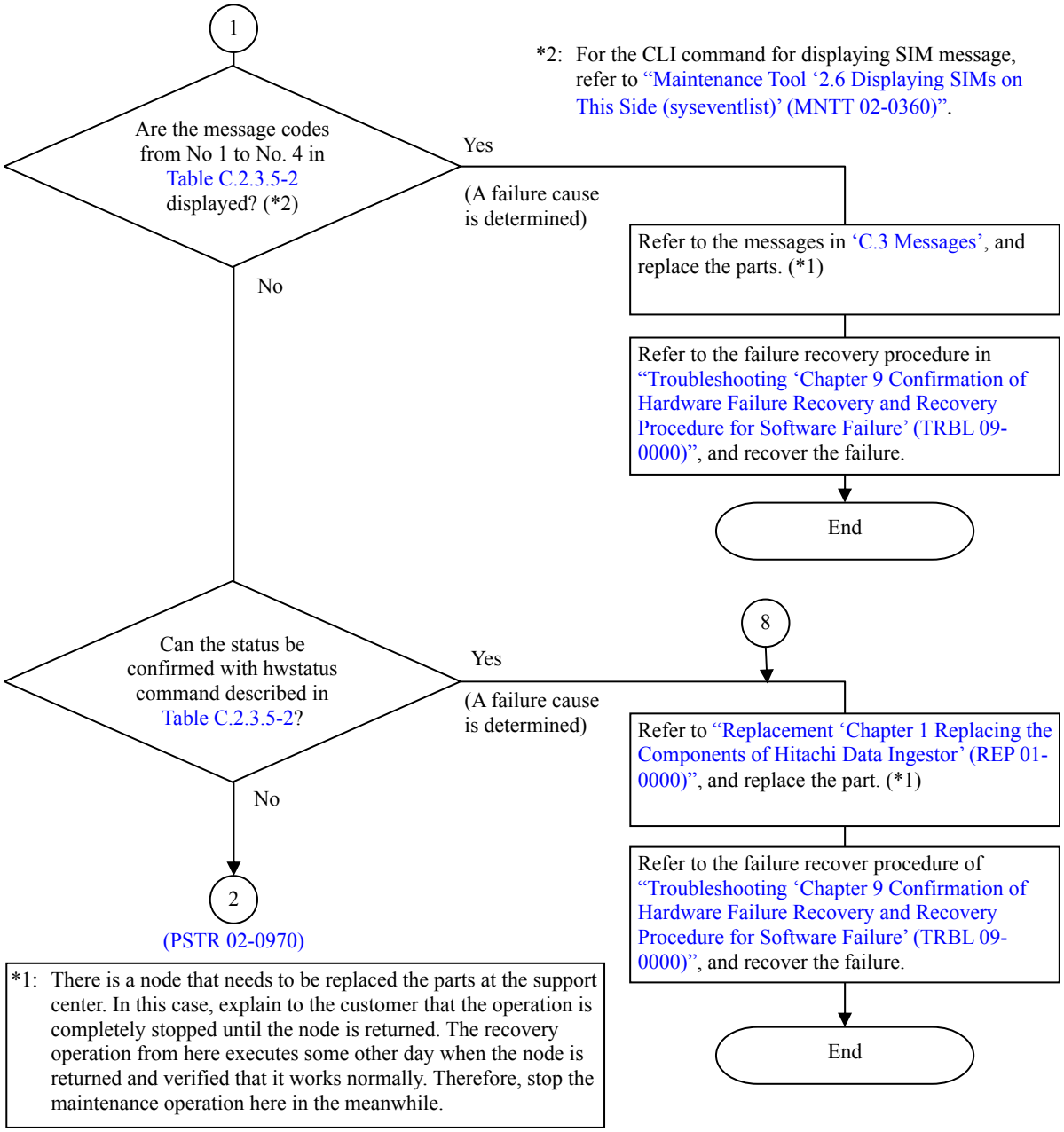


Figure C.2.3.5-1 Determining the node failure in the single node configuration (2/8)

Copyright © 2012, 2015, Hitachi, Ltd.

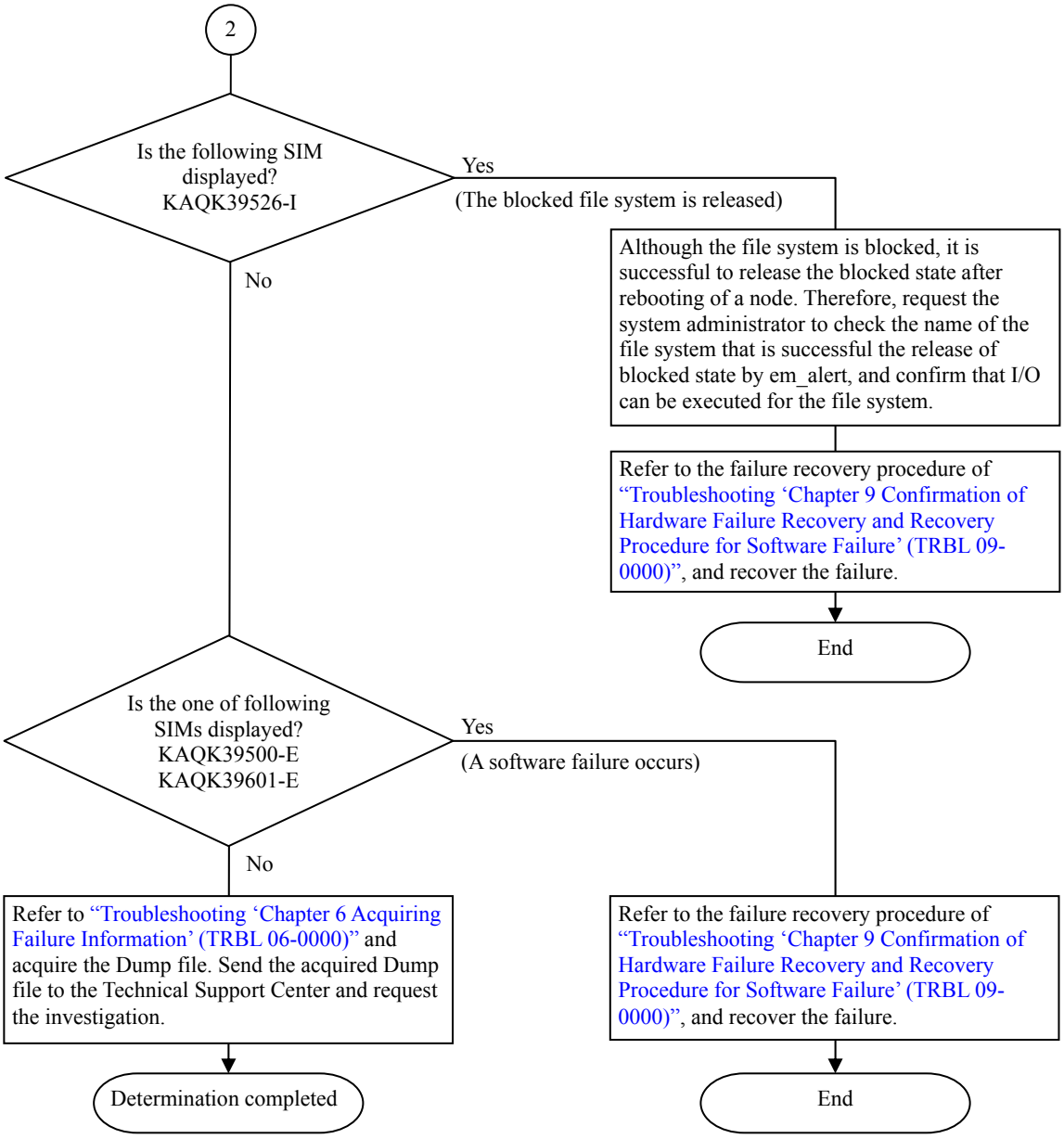


Figure C.2.3.5-1 Determining the node failure in the single node configuration (3/8)

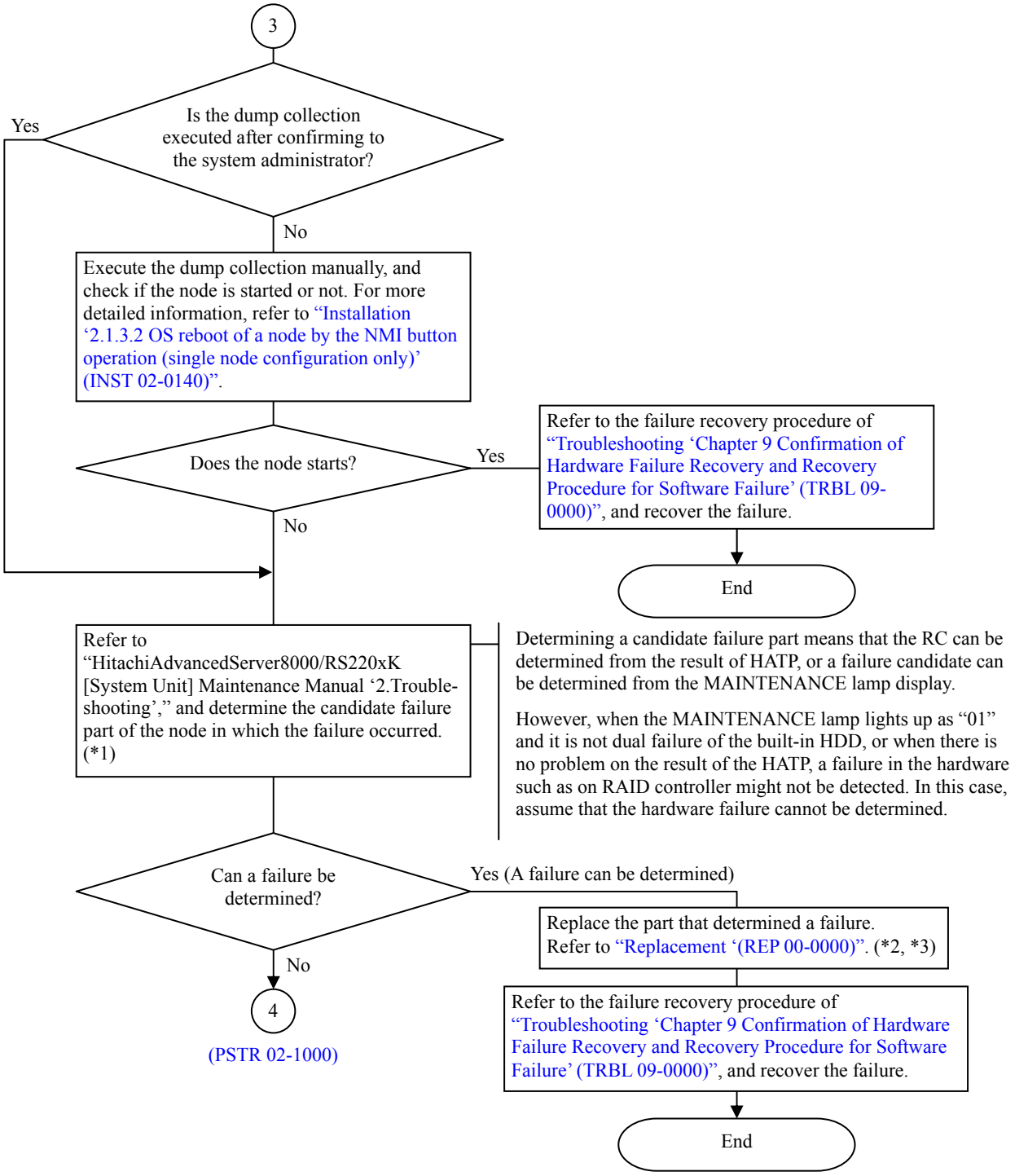
Copyright © 2011, 2013, Hitachi, Ltd.

Table C.2.3.5-2 Failed parts shown by SIM or LCD

#	SIM	Checking the status by the hwstatus command (*1)	Failed part
1	KAQG81003-W	Is the port status “Link down”?	On-board port, Extension NIC port, or cables (*2)
2	KAQK30801-E	—	Determine a failure part from the RC described in SIM and the continuous log (*3)
3	KAQK39504-E	Are the statuses of all ports of NIC “Link down”?	—
4	KAQK39527-E	—	Pool exhaustion (*4)
5	—	Is the status of BMC “Unknown!”?	BMC

*1: For the hwstatus command, refer to ‘B.3.1 Displaying the Hardware Status (hwstatus)’.
*2: When it is not recovered even if the cable is replaced, it is a port failure.
*3: For identifying a failure part from the RC and the continuous log, refer to “Hitachi Advanced Server8000/RS220xK [System Unit] Maintenance Manual”.
*4: Ask the system administrator to recover the pool exhaustion.

Copyright © 2011, 2014, Hitachi, Ltd.



*1: There is no problem to reboot the failed node for executing HATP.
*2: There is a node that needs to be replaced the parts at the support center. In this case, explain to the customer that the operation is completely stopped until the node is returned. The recovery operation from here executes some other day when the node is returned and verified that it works normally. Therefore, stop the maintenance operation here in the meanwhile.
*3: Make sure to collect Simple log by using HATP before the parts replacement.

Figure C.2.3.5-1 Determining the node failure in the single node configuration (4/8)

Copyright © 2011, 2014, Hitachi, Ltd.

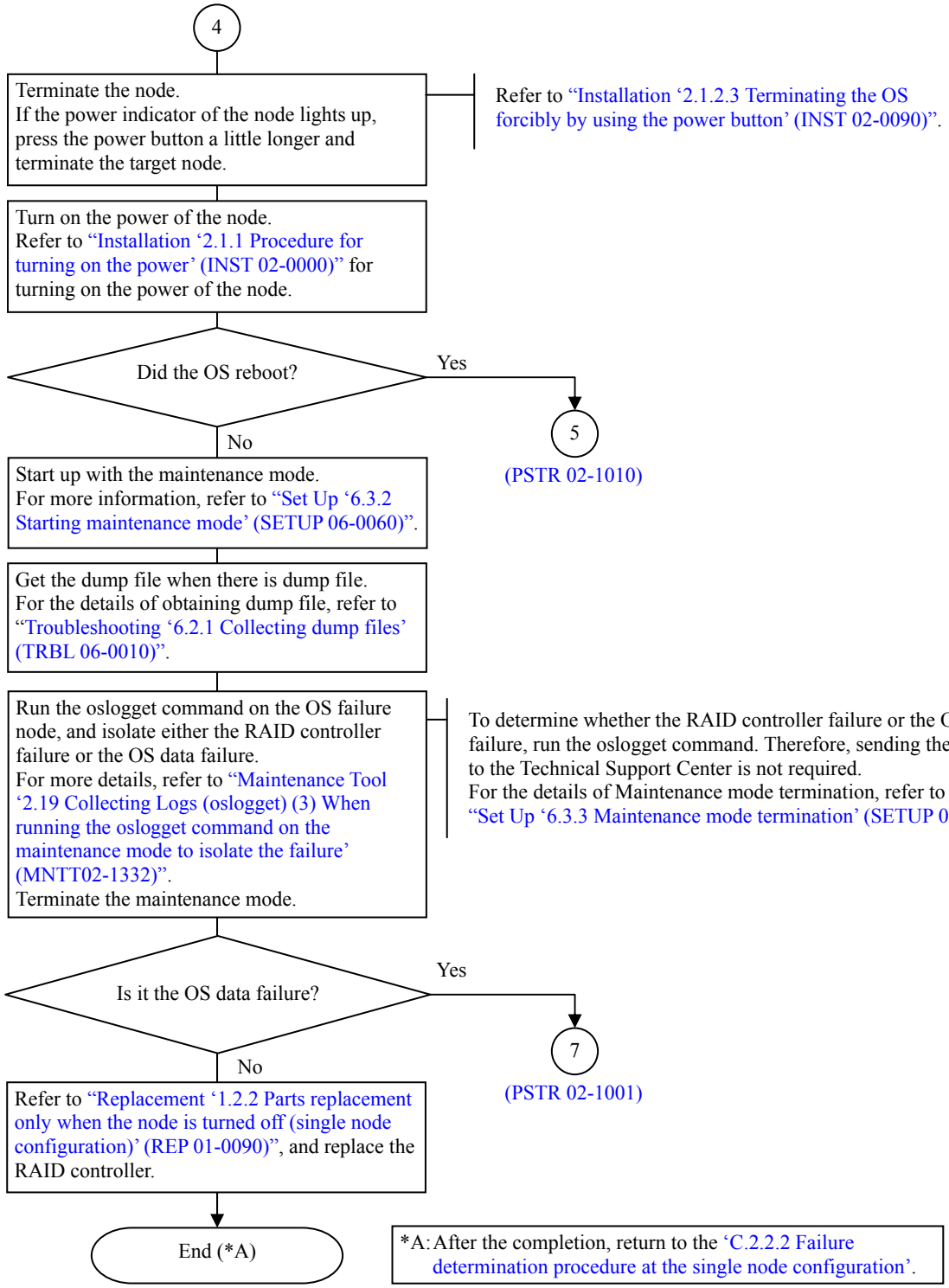


Figure C.2.3.5-1 Determining the node failure in the single node configuration (5/8)

Copyright © 2012, 2015, Hitachi, Ltd.

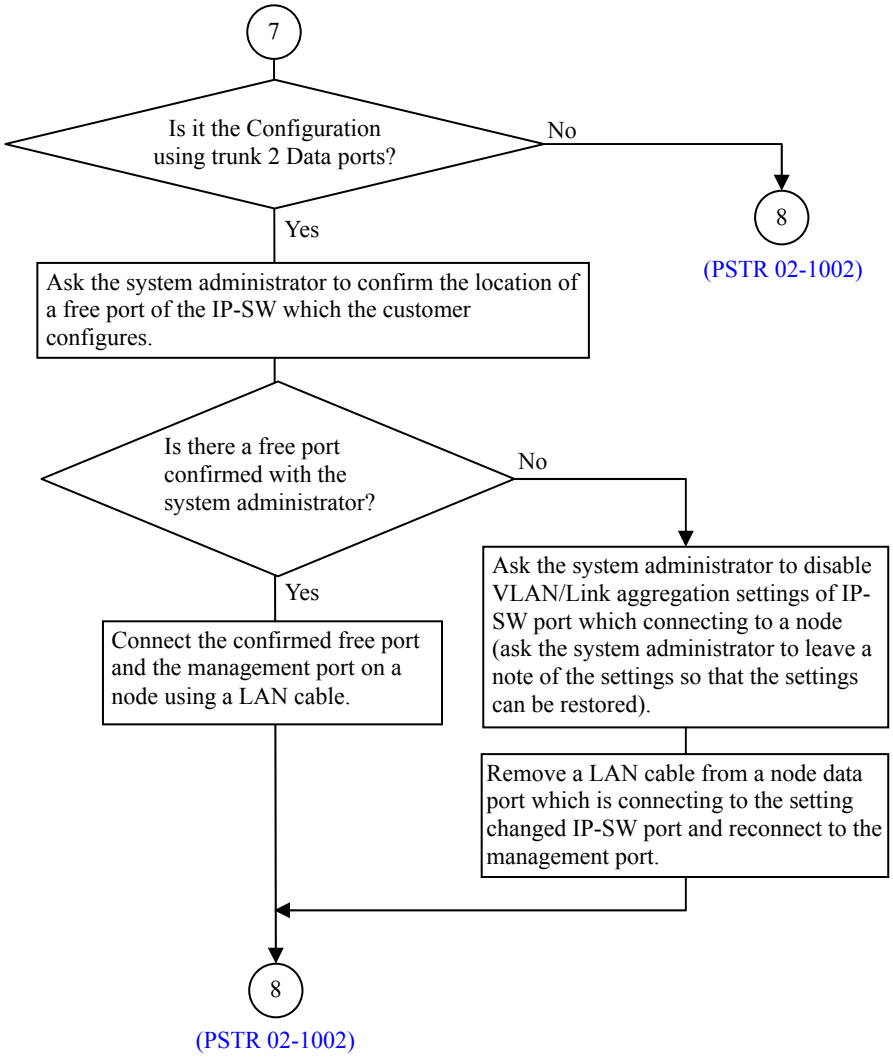
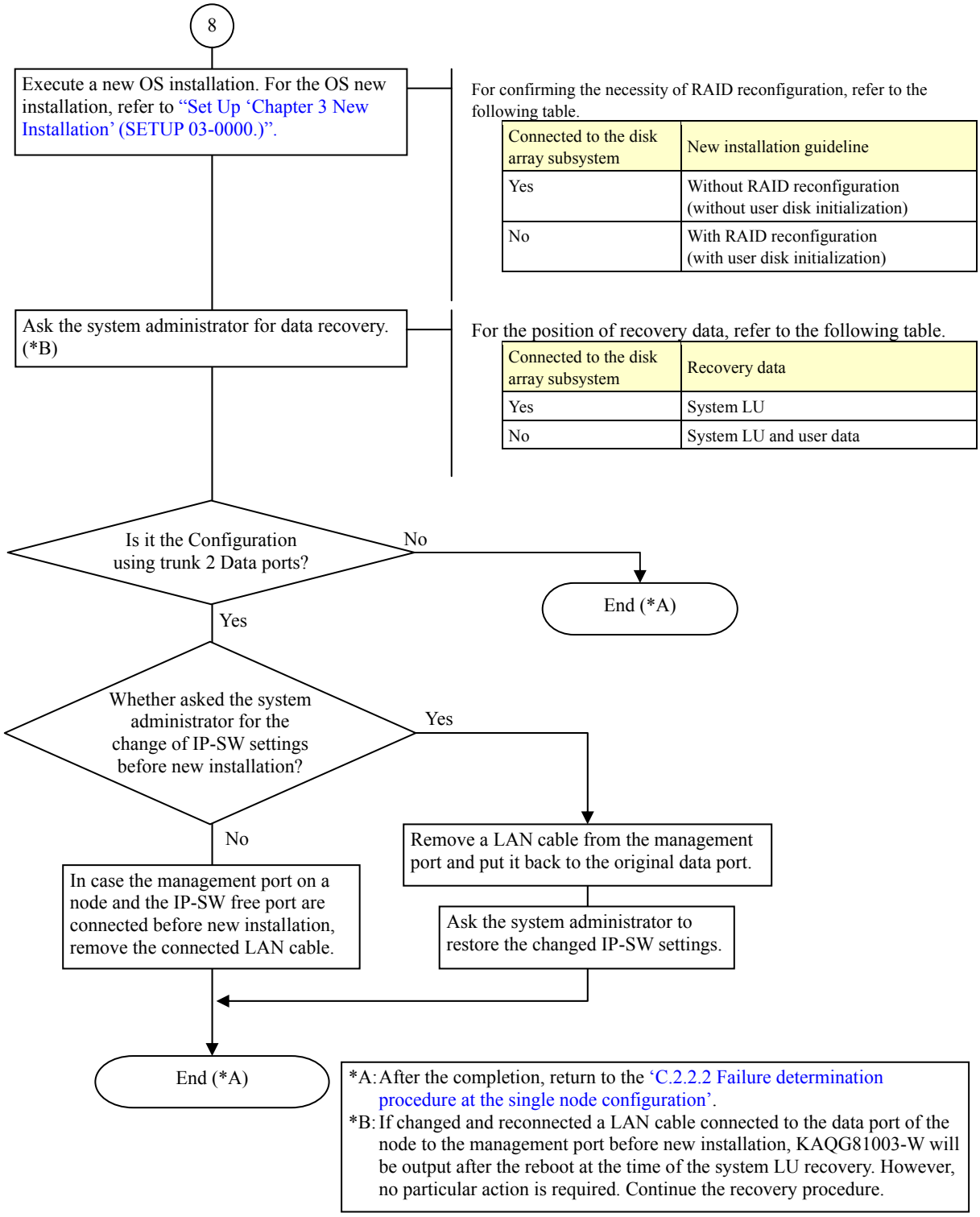


Figure C.2.3.5-1 Determining the node failure in the single node configuration (6/8)

Copyright © 2013, 2014, Hitachi, Ltd.

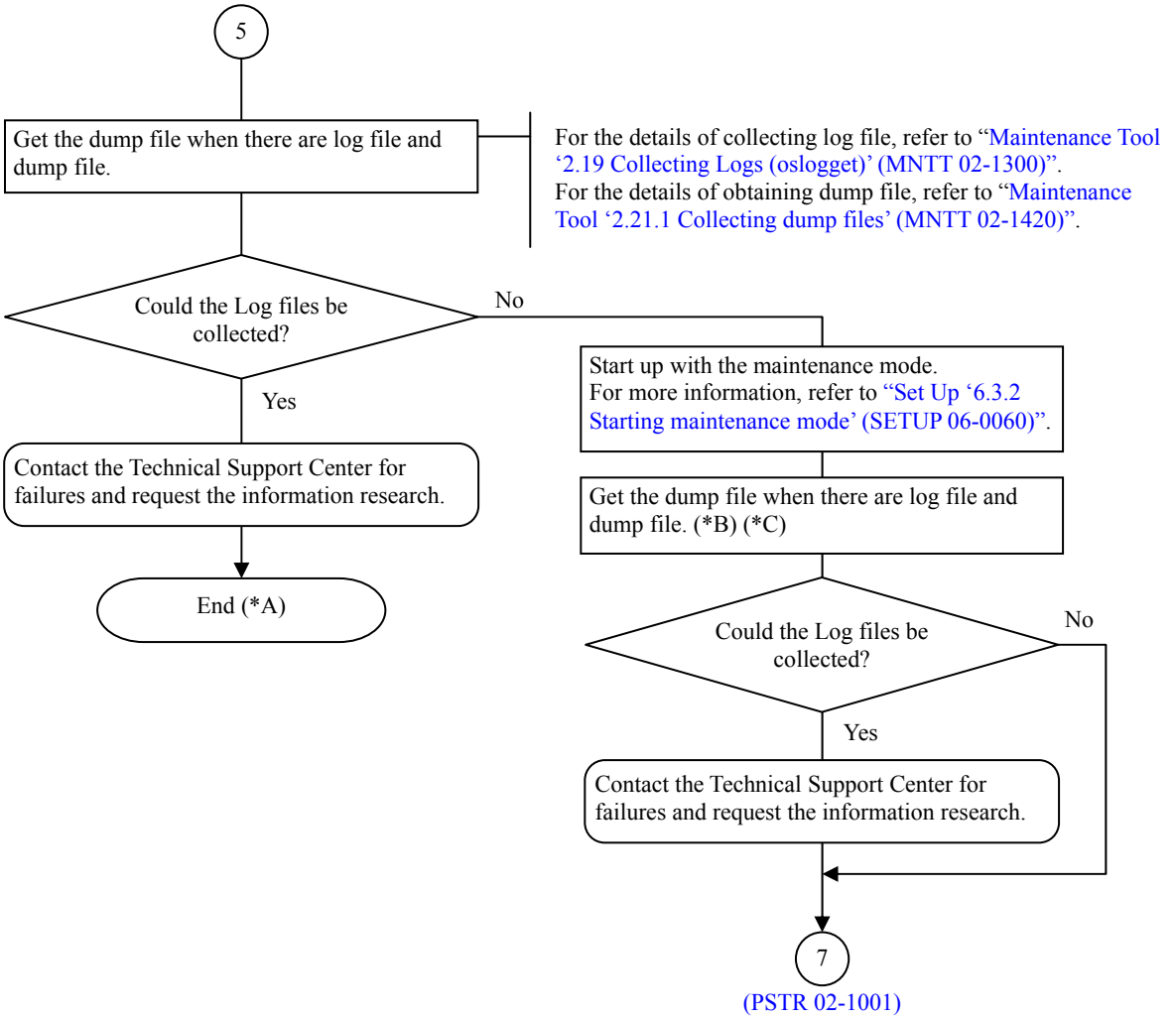


Connected to the disk array subsystem	New installation guideline
Yes	Without RAID reconfiguration (without user disk initialization)
No	With RAID reconfiguration (with user disk initialization)

Connected to the disk array subsystem	Recovery data
Yes	System LU
No	System LU and user data

Figure C.2.3.5-1 Determining the node failure in the single node configuration (7/8)

Copyright © 2013, Hitachi, Ltd.



*A: After the completion, return to the 'C.2.2.2 Failure determination procedure at the single node configuration'.
*B: For the details of collecting log file, refer to "Maintenance Tool '2.19 Collecting Logs (oslogget)' (MNTT 02-1300)".
For the details of obtaining dump file, refer to "Maintenance Tool '2.21.3 Confirm the existence of unconverted dump file (dumpcheck)' (MNTT 02-1461)".
*C: For the details of Maintenance mode termination, refer to "Set Up '6.3.3 Maintenance mode termination' (SETUP 06-0090)".

Figure C.2.3.5-1 Determining the node failure in the single node configuration (8/8)

Copyright © 2012, 2013, Hitachi, Ltd.

C.2.3.6 Determination of network failure

This section shows troubleshooting of SIM message from which it is difficult to determine a failure part in the case of displaying SIM about the network failure.

(1) In the case of the KAQG72012-W

Describe troubleshooting procedure as follow in the case of the “KAQG72012-W Communication via the main heartbeat cable was interrupted.” was displayed.

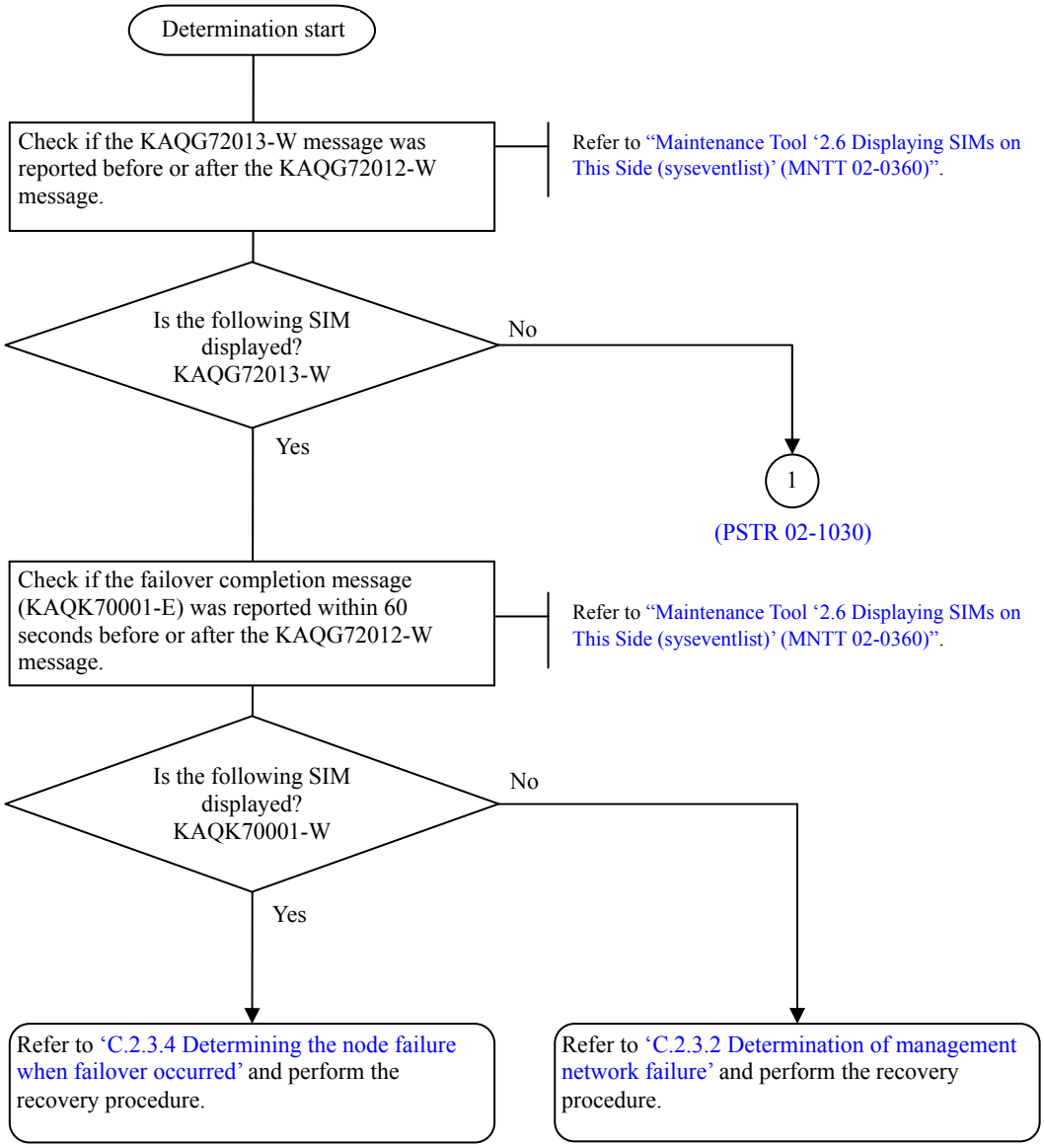


Figure C.2.3.6-1 Determination of network failure (KAQG72012-W) (1/2)

Copyright © 2016, Hitachi, Ltd.

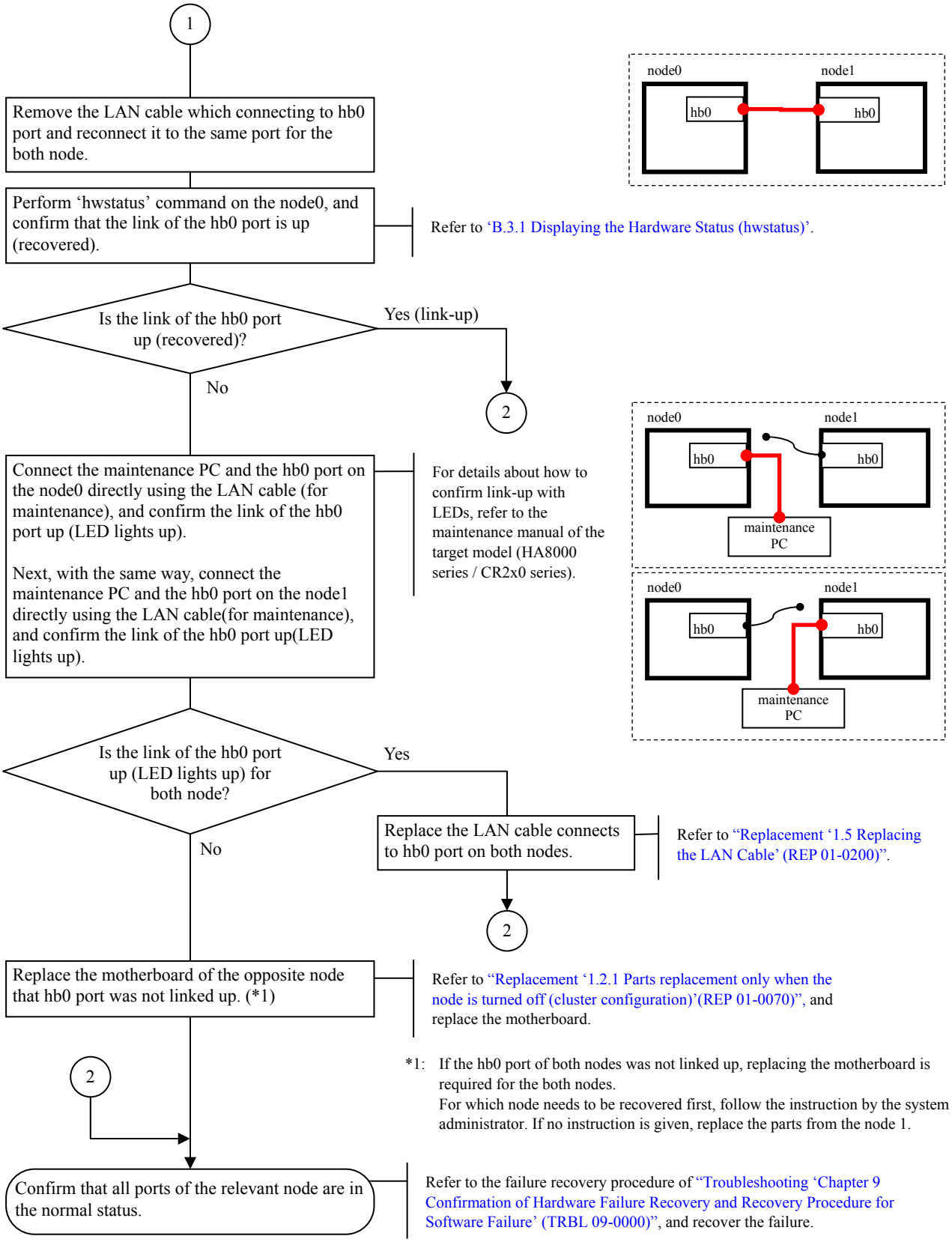


Figure C.2.3.6-1 Determination of network failure (KAQG72012-W) (2/2)

Copyright © 2016, Hitachi, Ltd.

(2) In the case of the KAQG81003-W

Describe troubleshooting procedure as follow in the case of the "KAQG81003-W Trunking driver: One or more subdevices are down. <*master-device-name*>:<*subdevice-name*>,<*subdevice-name*>…" was displayed.

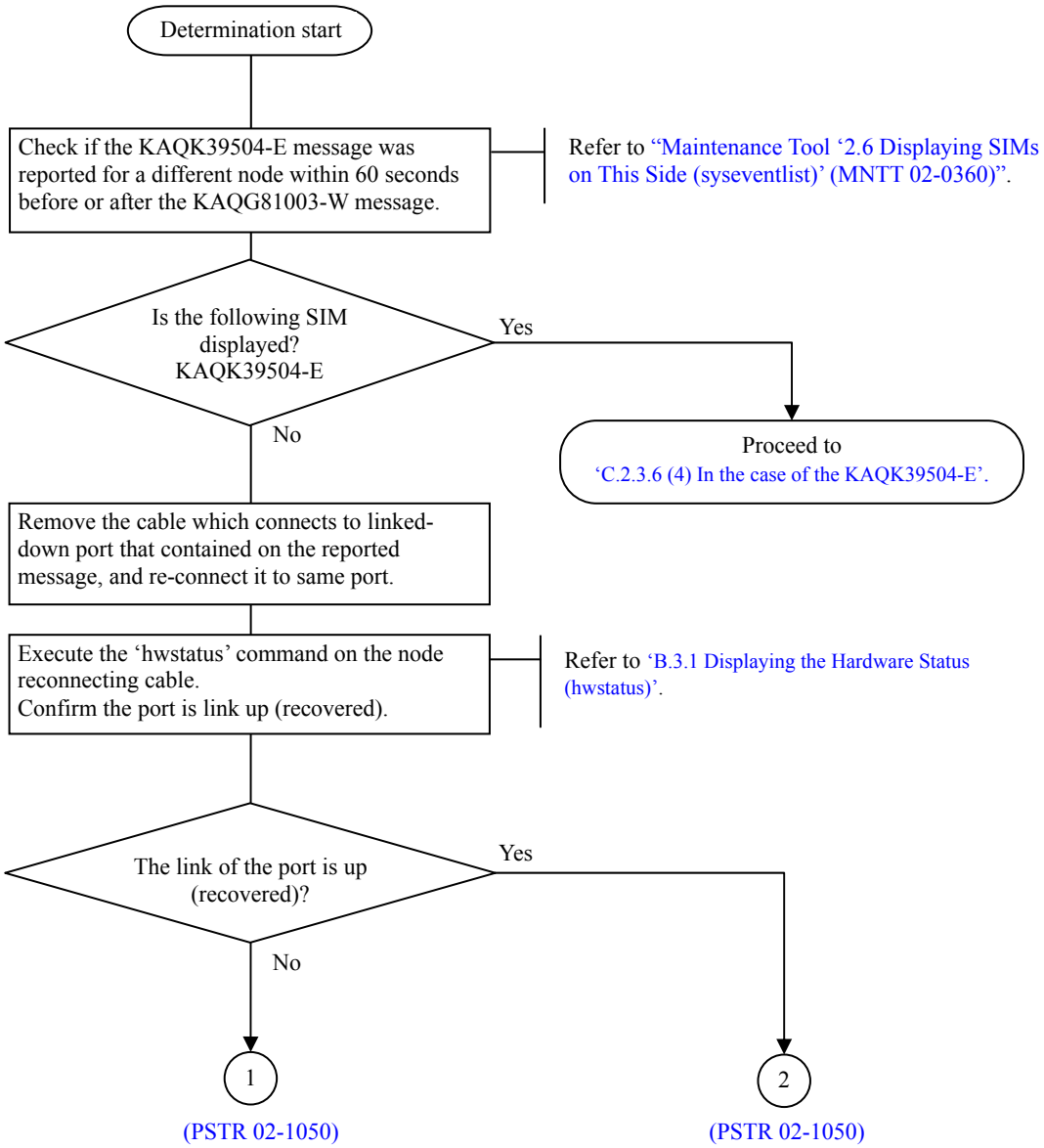


Figure C.2.3.6-2 Determination of network failure (KAQG81003-W) (1/2)

Copyright © 2016, Hitachi, Ltd.

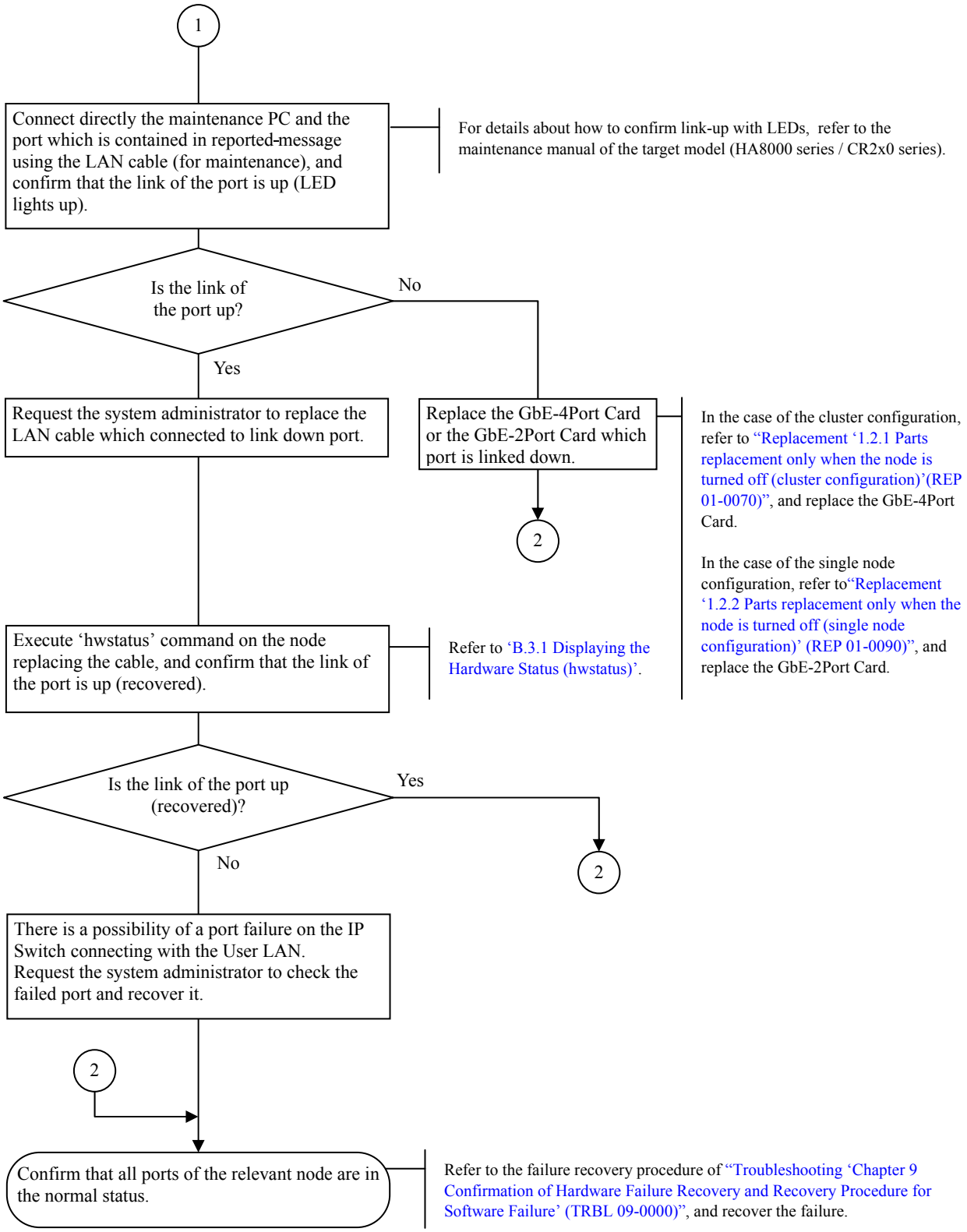


Figure C.2.3.6-2 Determination of network failure (KAQG81003-W) (2/2)

Copyright © 2016, Hitachi, Ltd.

(3) In the case of the KAQK36504-W

Describe troubleshooting procedure as follow in the case of the ”KAQK36504-W NIC: Link down detected(<*interface-name*>)” was displayed.

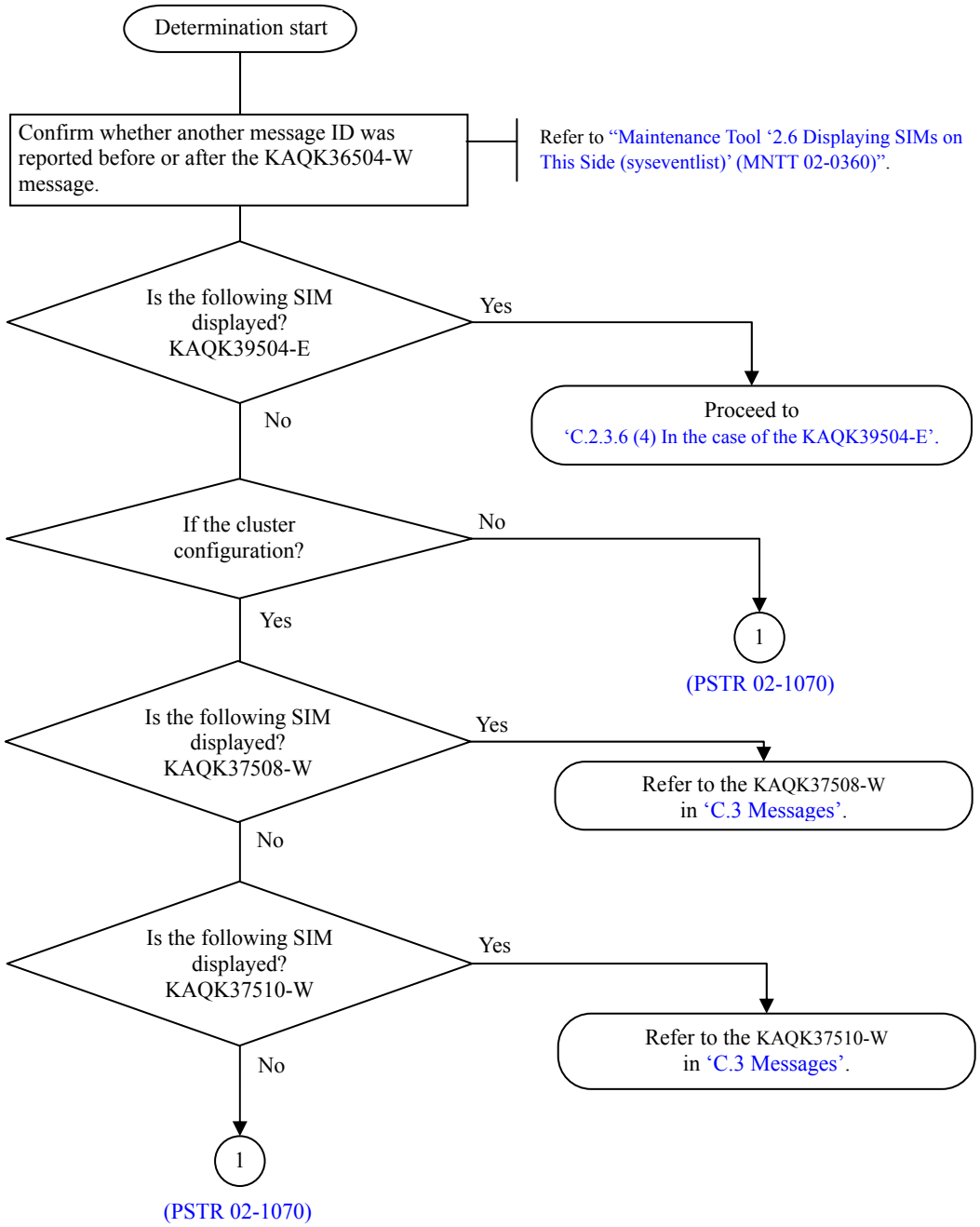


Figure C.2.3.6-3 Determination of network failure (KAQK36504-W) (1/3)

Copyright © 2016, Hitachi, Ltd.

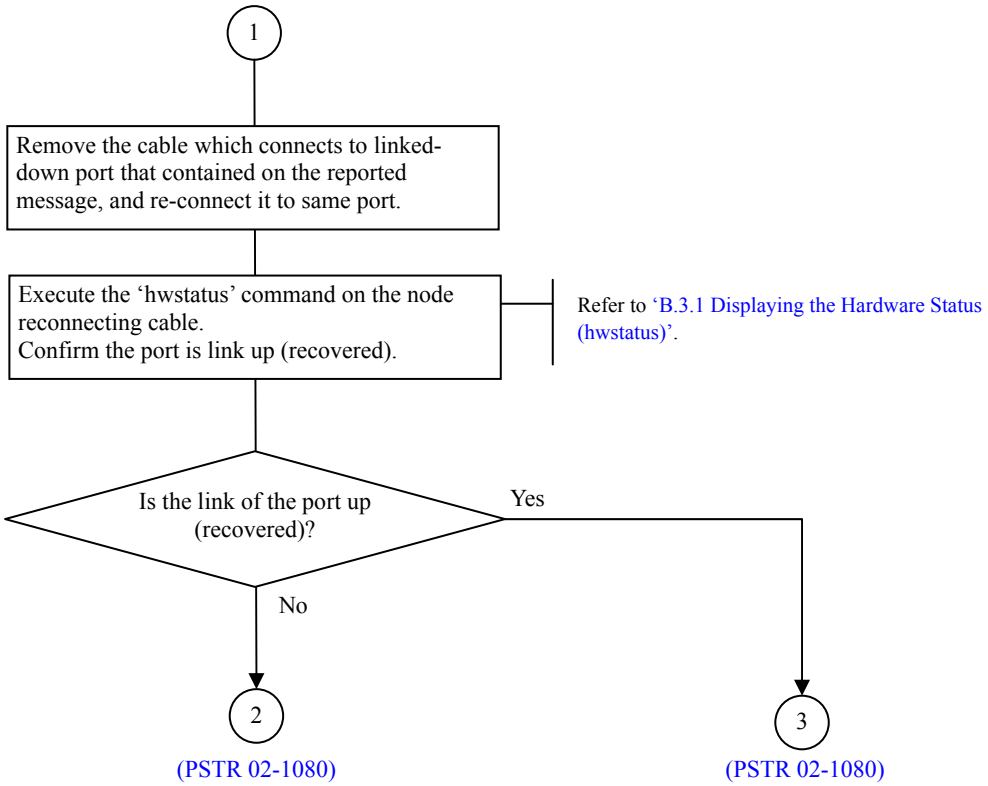


Figure C.2.3.6-3 Determination of network failure (KAQK36504-W) (2/3)

Copyright © 2016, Hitachi, Ltd.

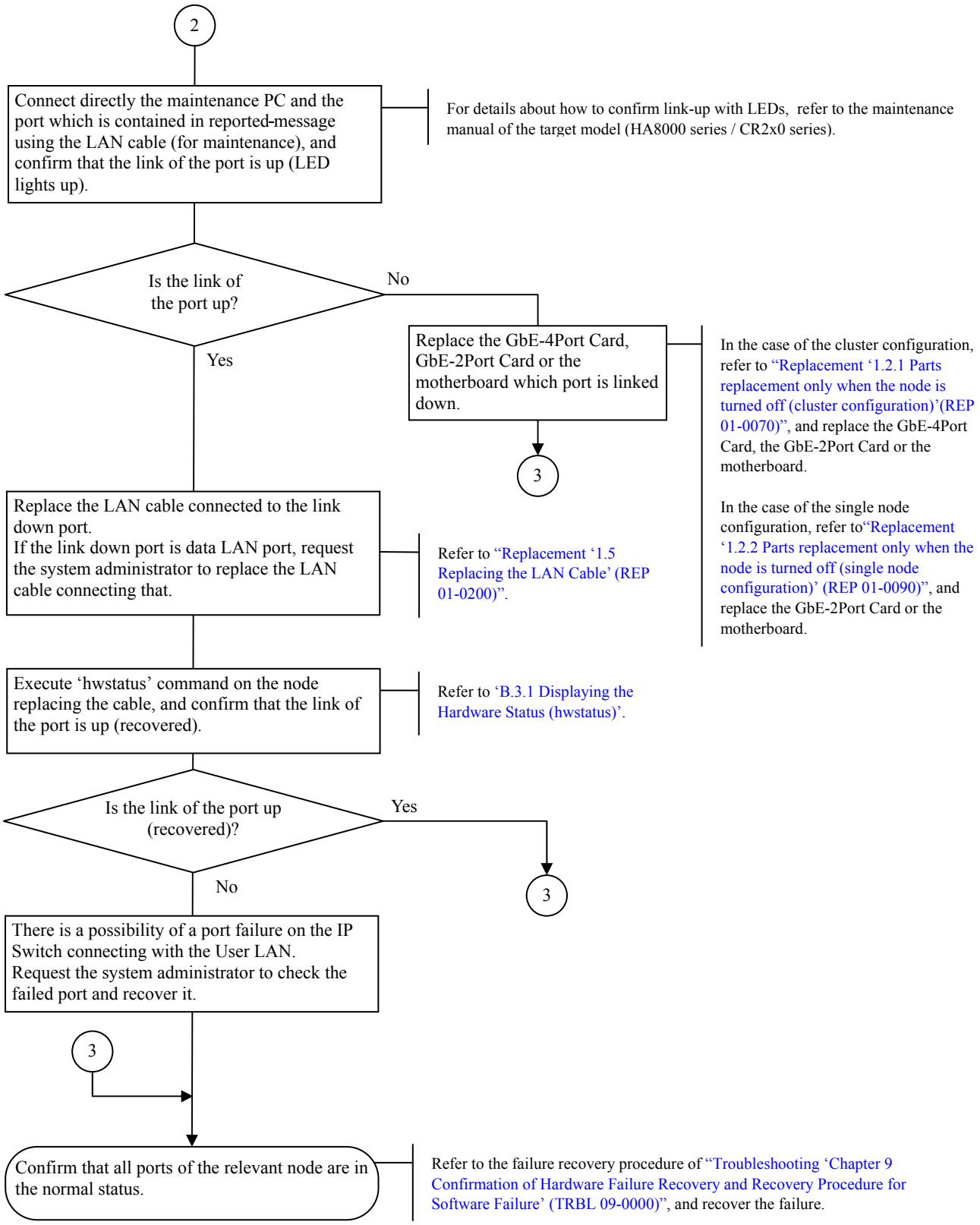


Figure C.2.3.6-3 Determination of network failure (KAQK36504-W) (3/3)

Copyright © 2016, Hitachi, Ltd.

(4) In the case of the KAQK39504-E

Describe troubleshooting procedure as follow in the case of the “KAQK39504-E Link down in Front-end LAN.” was displayed.

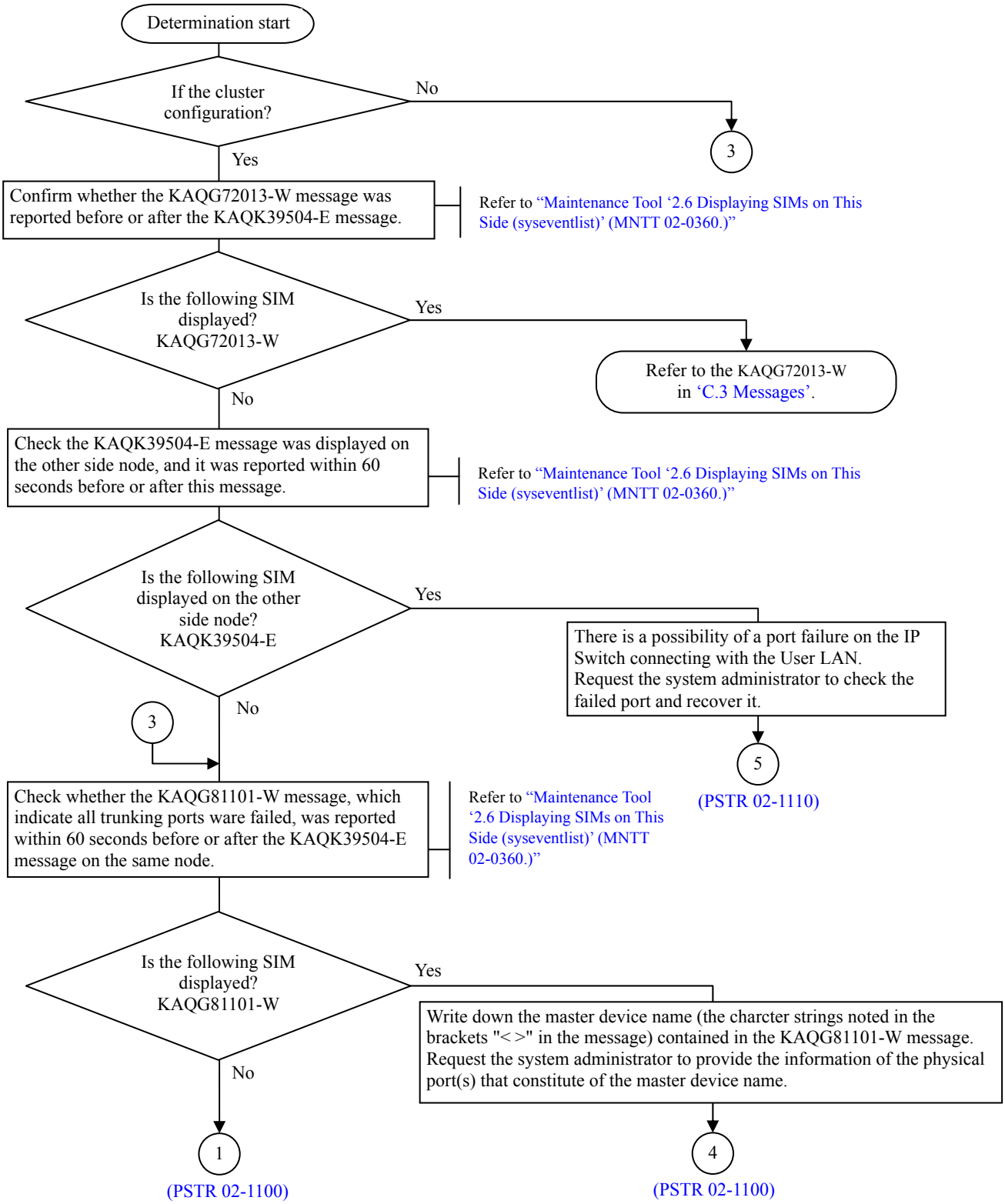


Figure C.2.3.6-4 Determination of network failure (KAQK39504-E) (1/3)

Copyright © 2016, Hitachi, Ltd.

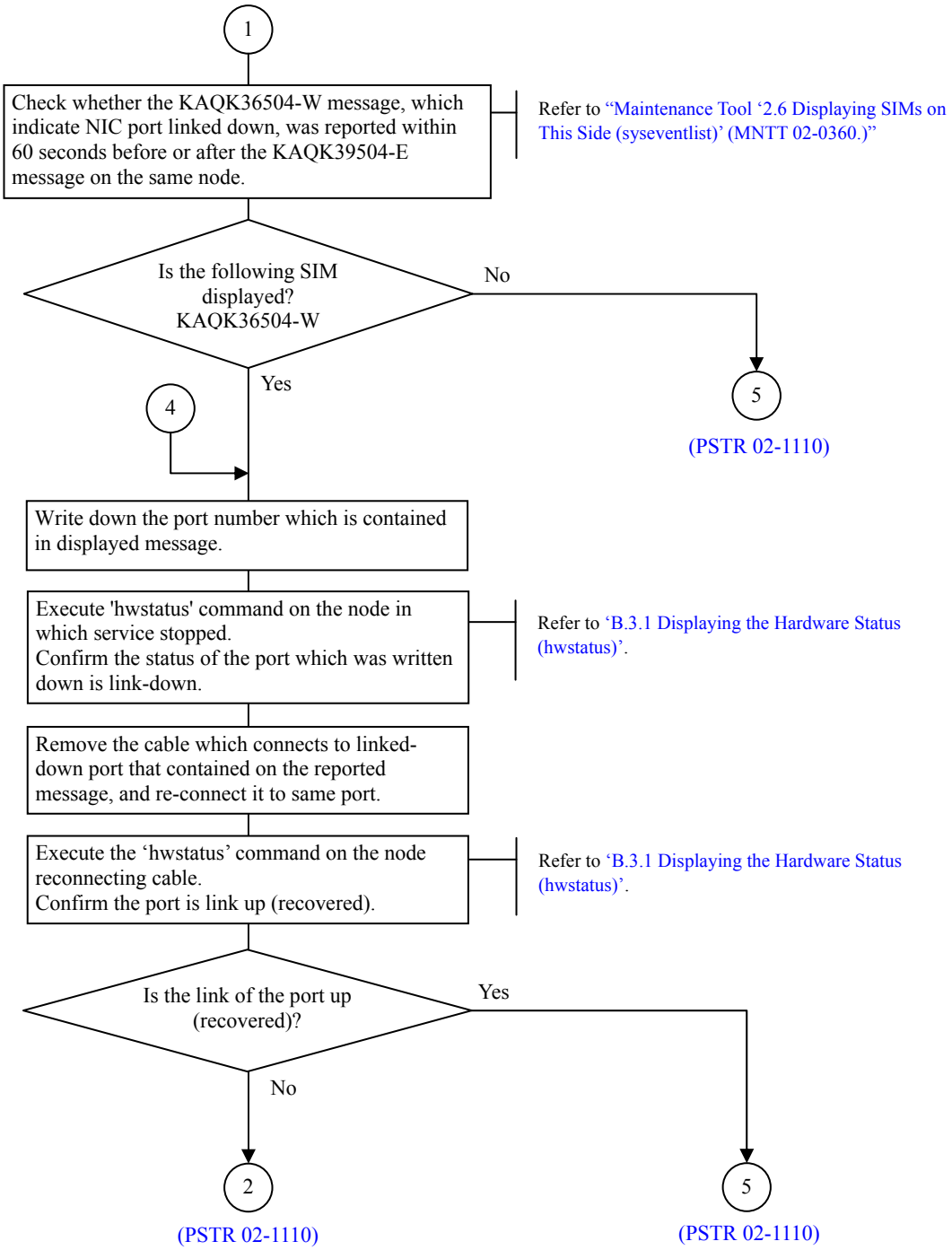


Figure C.2.3.6-4 Determination of network failure (KAQK39504-E) (2/3)

Copyright © 2016, Hitachi, Ltd.

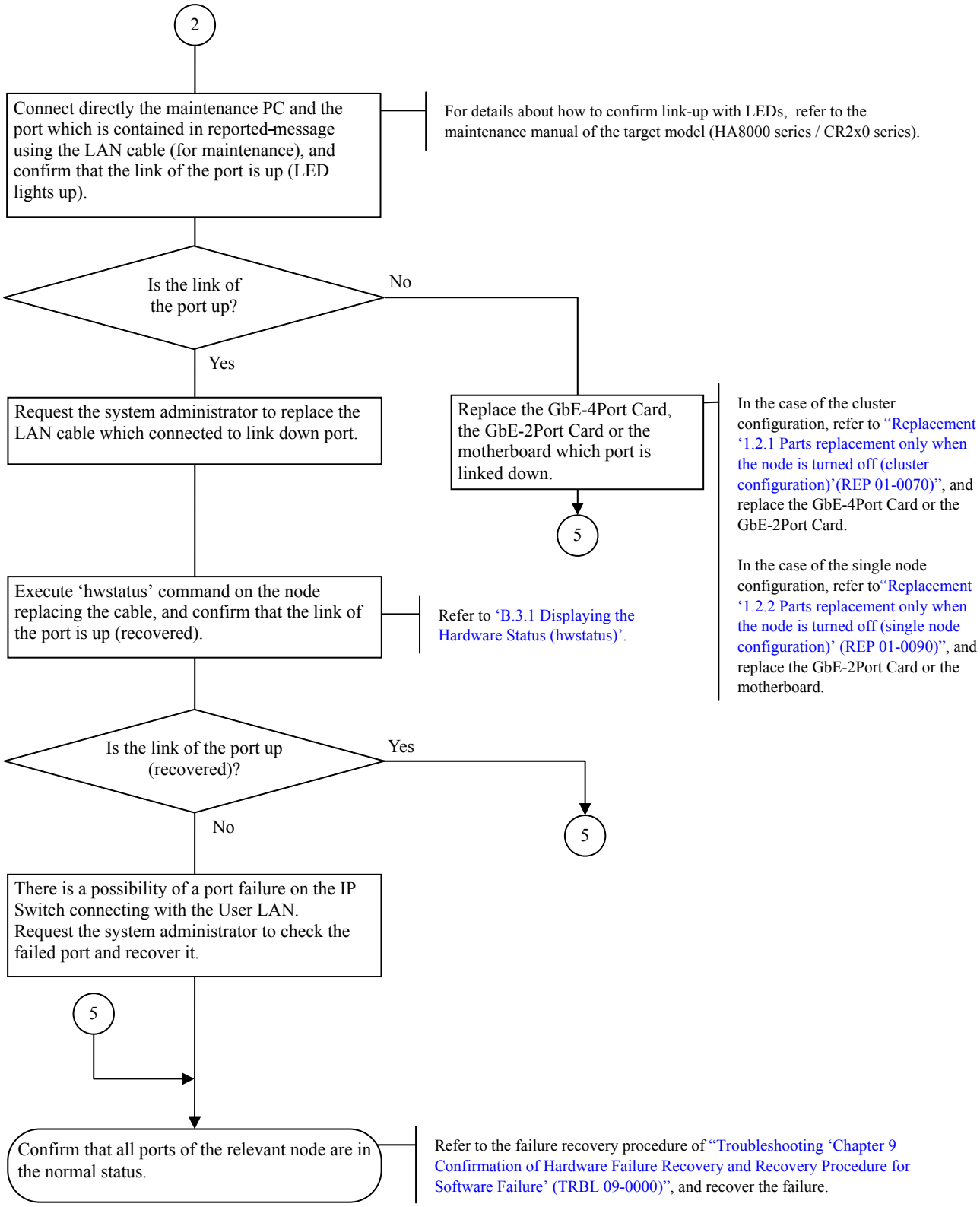


Figure C.2.3.6-4 Determination of network failure (KAQK39504-E) (3/3)

Copyright © 2016, Hitachi, Ltd.

C.2.4 Diagnosis for OS Boot Failure

This section describes how to diagnose when the replaced part failure or other failure cause the OS boot failure after parts replacement operation.

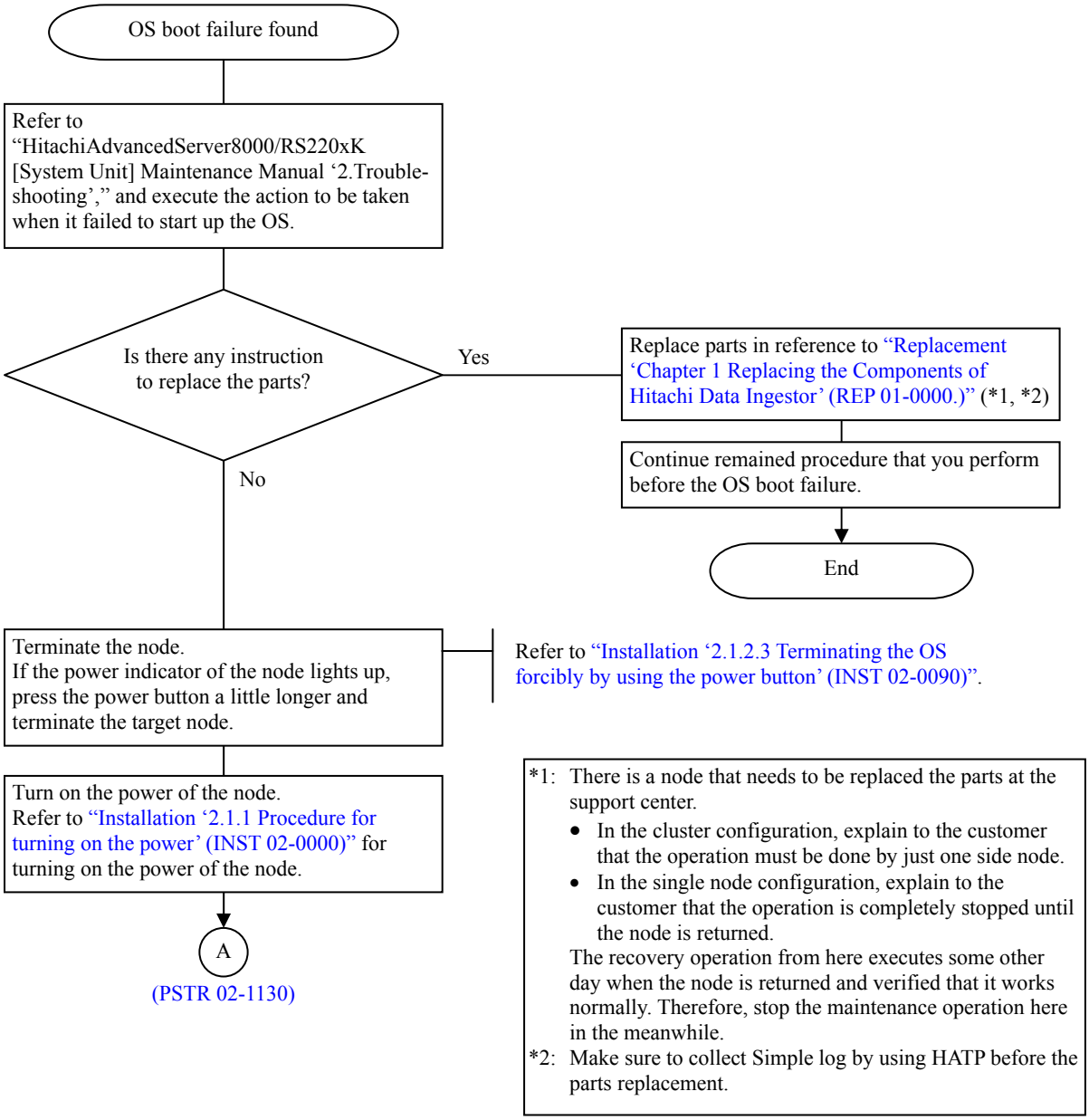


Figure C.2.4-1 Flow of Diagnosis for OS boot failure (1/5)

Copyright © 2012, 2016, Hitachi, Ltd.

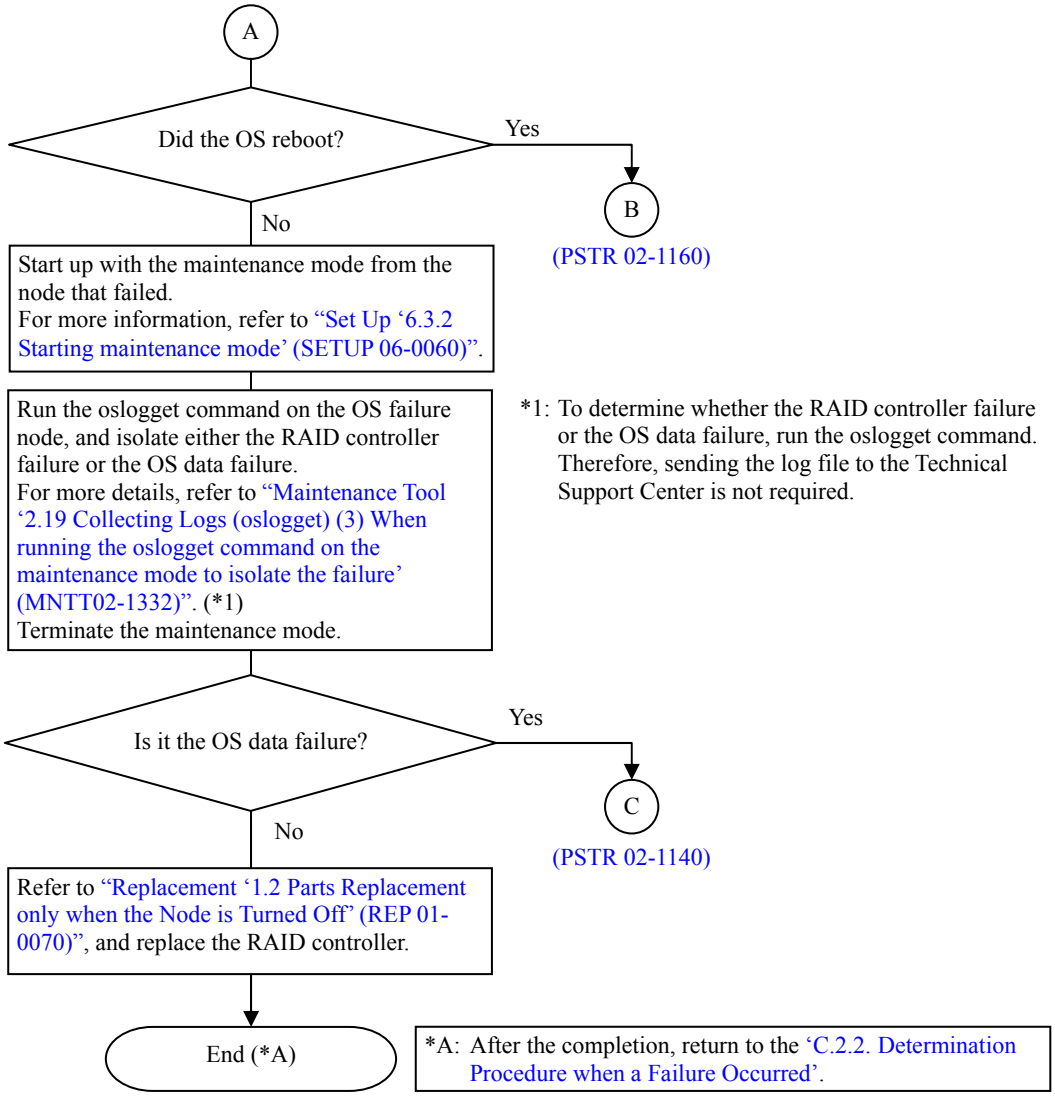


Figure C.2.4-1 Flow of Diagnosis for OS boot failure (2/5)

Copyright © 2012, 2016, Hitachi, Ltd.

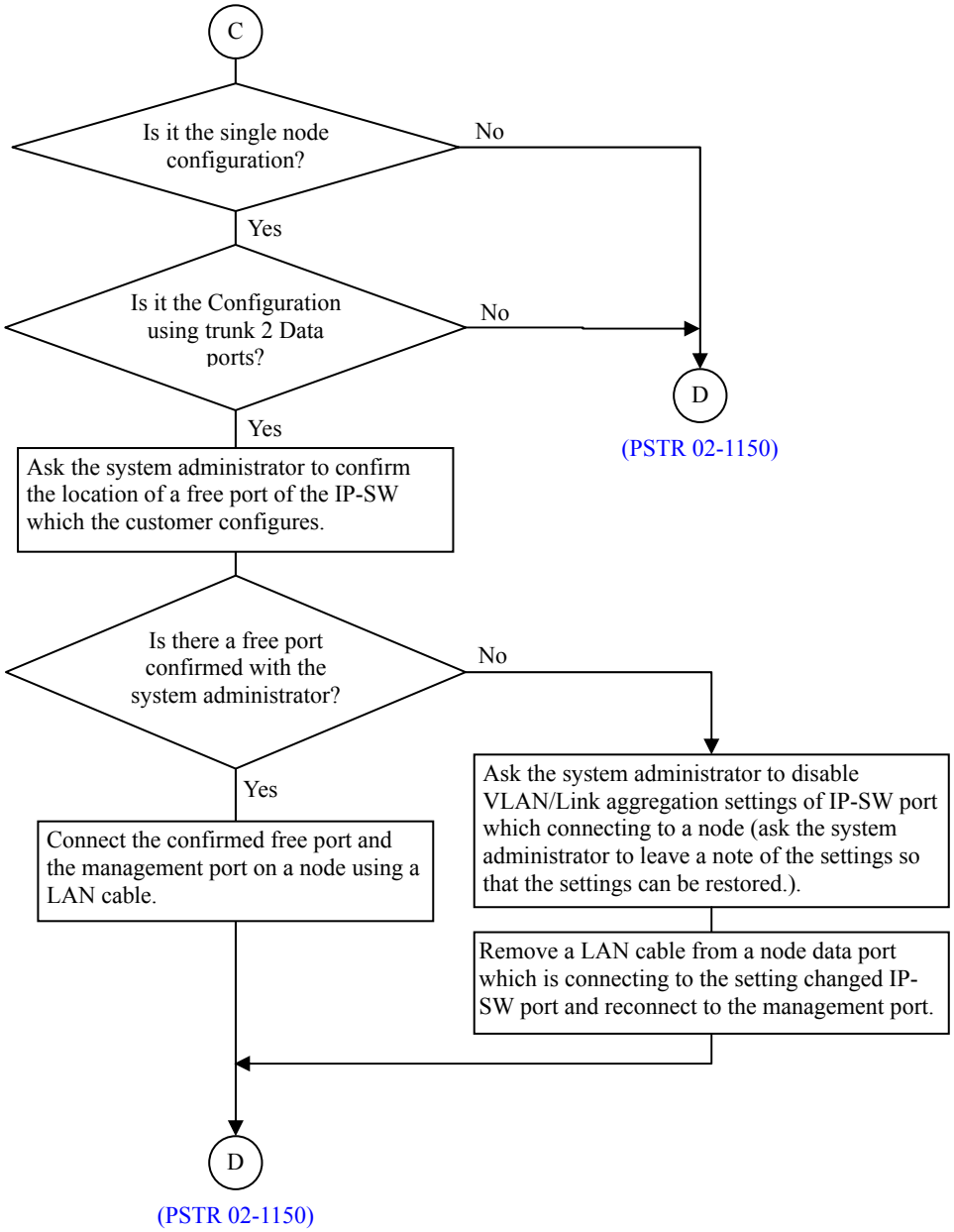
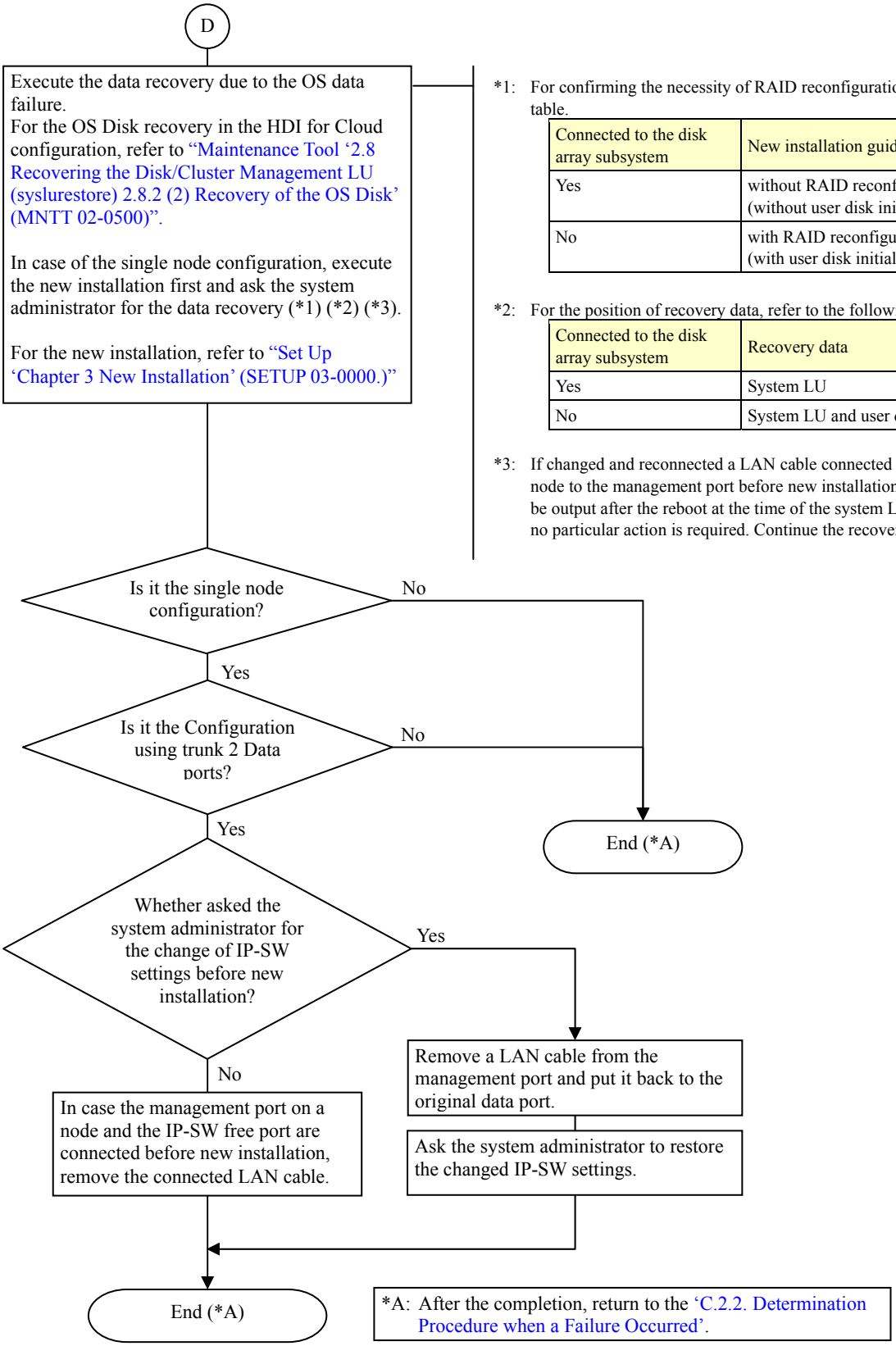


Figure C.2.4-1 Flow of Diagnosis for OS boot failure (3/5)

Copyright © 2013, 2016, Hitachi, Ltd.



*1: For confirming the necessity of RAID reconfiguration, refer to the following table.

Connected to the disk array subsystem	New installation guideline
Yes	without RAID reconfiguration (without user disk initialization)
No	with RAID reconfiguration (with user disk initialization)

*2: For the position of recovery data, refer to the following table.

Connected to the disk array subsystem	Recovery data
Yes	System LU
No	System LU and user data

*3: If changed and reconnected a LAN cable connected to the data port of the node to the management port before new installation, KAQG81003-W will be output after the reboot at the time of the system LU recovery. However, no particular action is required. Continue the recovery procedure.

Figure C.2.4-1 Flow of Diagnosis for OS boot failure (4/5)

Copyright © 2013, 2016, Hitachi, Ltd.

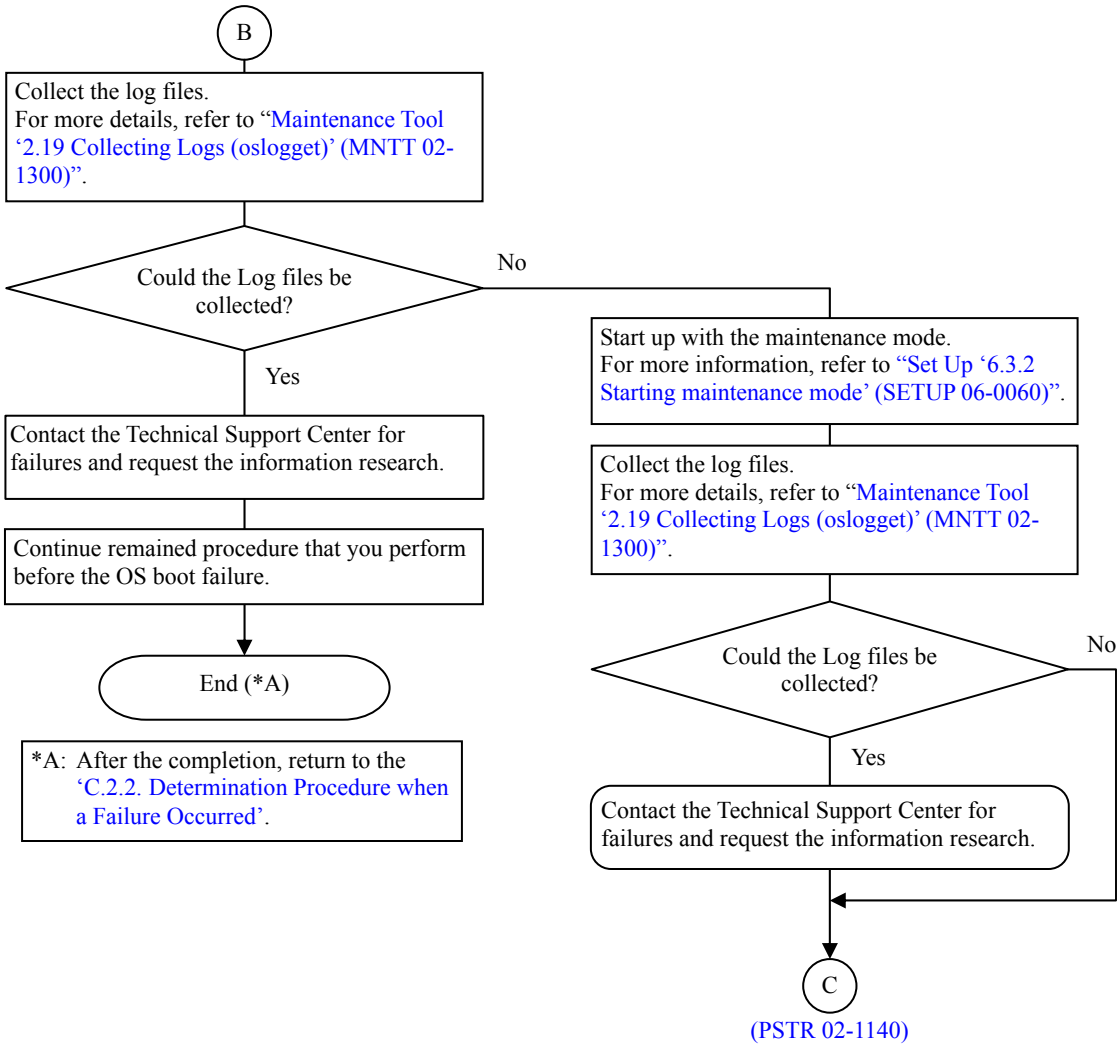


Figure C.2.4-1 Flow of Diagnosis for OS boot failure (5/5)

Copyright © 2011, 2016, Hitachi, Ltd.

This page is for editorial purpose only.

Copyright © 2013, 2016, Hitachi, Ltd.

CONTENTS

C.3 Messages

C.3.1 SIM Messages

C.3.2 LCD Display Message Code

C.3.3 KAQX Messages

Copyright © 2011, 2015, Hitachi, Ltd.

This page is for editorial purpose only.

Copyright © 2011, 2013, Hitachi, Ltd.

C.3 Messages

This chapter describes messages.

C.3.1 SIM Messages

SIM messages detected by HDI and the recovery methods are described below.

Table C.3.1-1 Message IDs (70000s)

Message ID	Message text	Description	Recovery method	Reference Page
KAQG70000-E	Failover started, Node-<*node-number*> [(virtual server ID = <*virtual-server-ID*>)]	This message reports that a failover started at <*#node*>. When the target failover is Virtual Server, <*virtual-server-ID*> is output in brackets “( )”.	—	—
KAQG70001-E	Failover ended, Node-<*node-number*> [(virtual server ID = <*virtual-server-ID*>)]	This message reports that a failover was completed at <*#node*>. When the target failover is Virtual Server, <*virtual-server-ID*> is output in brackets “( )”.	—	—
KAQG72001-E	Failover ended(Move failed),Node-<*node-number*>[(virtual server ID = <*virtual-server-ID*>)]	This message reports that a failover failed. When the target failover is Virtual Server, <*virtual-server-ID*> is output in brackets “( )”.	Perform the recovery procedure according to Troubleshooting “Chapter 1 Method of Local Initial Motion according to Maintenance Request”.	“Troubleshooting ‘Chapter 1 Method of Local Initial Measures According to Maintenance Request’ (TRBL 01-0000)”
KAQG72011-E	Synchronization of the cluster information might become invalid.	This message reports that a failure occurred in the internal database of the cluster.	Perform the recovery procedure according to Troubleshooting “Chapter 1 Method of Local Initial Motion according to Maintenance Request”.	“Troubleshooting ‘Chapter 1 Method of Local Initial Measures According to Maintenance Request’ (TRBL 01-0000)”

Copyright © 2011, 2013, Hitachi, Ltd.

Message ID	Message text	Description	Recovery method		Reference Page
KAQG72012-W	Communication via the main heartbeat cable was interrupted.	A failure occurred in the main heartbeat cable.	Follow the determination flowchart of Troubleshooting ‘C.2.3.6 Determination of network failure (1) In the case of the KAQG72012-W’.		‘C.2.3.6 Determination of network failure (1) In the case of the KAQG72012-W’
KAQG72013-W	Communication via the sub heartbeat cable was interrupted.	A failure occurred in the sub heartbeat cable.	①	Check if the KAQG72012-W message was reported before or after the KAQG72013-W message. • If it was reported, two heartbeat cables are disconnected (Link down). Proceed to step②. • If it was not reported, proceed to step③.	—
			②	Check if the failover completion message (KAQK70001-E) was reported within 60 seconds before or after this message. • If it is reported, refer to ‘C.2.3.4 Determining the node failure when failover occurred,’ and then execute the failure determination. • If it is not confirmed, refer to ‘C.2.3.2 Determination of management network failure’ and perform the recovery procedure.	‘C.2.3.4 Determining the node failure when failover occurred’ ‘C.2.3.2 Determination of management network failure’
			③	A failure occurred on the way of connecting maintenance LAN port of the node. Follow the procedure of ‘C.2.2 Determination Procedure when a Failure Occurred’.	‘C.2.2 Determination Procedure when a Failure Occurred’
KAQG72014-I	Communication via the main heartbeat cable was restored.	The main heartbeat cable has recovered.	—		—
KAQG72015-I	Communication via the sub heartbeat cable was restored.	The sub heartbeat cable has recovered.	—		—

Copyright © 2012, 2016, Hitachi, Ltd.

Message ID	Message text	Description	Recovery method	Reference Page
KAQG72026-E	The resource group on the other node will be forcibly failed over to clear the DISABLE state of the cluster.	Automatic forced failover occurred.	A failure occurs on the power source or on the heartbeat channel and the reset channel connecting the both nodes. Go to 'C.2.2 Determination Procedure when a Failure Occurred', and then execute the troubleshooting.	'C.2.2 Determination Procedure when a Failure Occurred'
KAQG72027-E	The OS will restart to clear the DISABLE state of the cluster.	Automatic forced failover occurred on the other side node.	① Check if the KAQG72026-E message was reported for the other side node at the same period of time. •If it is reported, a failure has been occurred on the routes of heartbeat and reset that are connecting both nodes. Refer to "Message IDs (KAQG72026-E)". •If it was not reported, or the other side node is stopped, proceed to step②.	Message IDs (KAQG72026-E)
			② It might be interrupted the process of forced failover due to another failure. Refer to Troubleshooting "Chapter 6 Acquiring Failure Information", and get the troubleshooting information. After that, contact to the technical support center.	"Troubleshooting 'Chapter 6 Acquiring Failure Information' (TRBL 06-0000)"
KAQG72028-W	The forced failover state will be cleared because the problem on the other node has been resolved.	The state of automatic forced failover is recovered.	—	—
KAQG72029-E	To clear the forced failover state, an attempt was made to restart the OS of the other node, but the attempt failed.	Resetting of the other side node failed at the time of recovering the state of forced failover.	The heartbeat channel that connected both nodes of a cluster where was in the state of automatic forced failover is recovered, but the reset process for the other side node has failed because there was still a failure on the reset channel. Go to 'C.2.2 Determination Procedure when a Failure Occurred', and then execute the troubleshooting.	'C.2.2 Determination Procedure when a Failure Occurred'
KAQG72030-E	To clear the forced failover state, an attempt was made to release access protection on one more LUs, but the attempt failed.	Releasing of the LU access protection failed at the time of recovering the state of forced failover.	The heartbeat channel that connected both nodes of a cluster in the state of automatic forced failover is recovered, but the release of LU access protection has failed. Refer to Troubleshooting "5.3 Measures when Releasing the LU Access Protection Failed", and execute the recovery procedure.	"Troubleshooting '5.3 Measures when Releasing the LU Access Protection Failed' (TRBL 05-0530)"

Copyright © 2012, 2016, Hitachi, Ltd.

Table C.3.1-2 Message IDs (80000s)

Message ID	Message text	Description	Recovery method	Reference Page
KAQG81003-W	Trunking driver: One or more subdevices are down. *<master-device-name>:<subdevice-name>,<subdevice-name>…*	Links of the reported driver are combined (i.e. the number of links increases or decreases).	Follow the determination flowchart of Troubleshooting 'C.2.3.6 Determination of network failure (2) In the case of the KAQG81003-W'.	'C.2.3.6 Determination of network failure (2) In the case of the KAQG81003-W'
KAQG81004-I	Trunking driver: The subdevices that were down have been recovered. *<master-device-name>*: *<subdevice-name>*, *<subdevice-name>…*	Links of the reported driver are combined (i.e. down links have recovered).	—	—
KAQG81101-W	Trunking driver: The master device *<link-combined-device-name>* is down because all the sub-device were down.	Failures occurred in all ports of the combined links.	In the case of the cluster configuration, check if the KAQG70001-E message was reported within 60 seconds before or after this message. • If it is confirmed, follow the determination flowchart of Troubleshooting 'C.2.3.6 Determination of network failure (4) In the case of the KAQK39504-E'. • If it is not confirmed, there is a possibility of a port failure on the IP Switch connecting with the User LAN. Request the system administrator to check the failed port and recover it. After the IP Switch recovery, refer to the failure recovery procedure of Troubleshooting "Chapter 9 Confirmation of Hardware Failure Recovery and Recovery Procedure for Software Failure" and confirm that all ports of the relevant node are in the normal status. In the case of the single node configuration, follow the determination flowchart of Troubleshooting 'C.2.3.6 Determination of network failure (4) In the case of the KAQK39504-E'.	'C.2.3.6 Determination of network failure (4) In the case of the KAQK39504-E' "Troubleshooting 'Chapter 9 Confirmation of Hardware Failure Recovery and Recovery Procedure for Software Failure' (TRBL 09-0000)"
KAQK81102-I	Trunking driver: The sub-devices that were down have recovered, and the master device <link-combined-device> has recovered.	All ports of the combined links have recovered.	—	—

Copyright © 2012, 2016, Hitachi, Ltd.

Table C.3.1-3 Message IDs (30000s)

Message ID	Message text	Description	Recovery method		Reference Page
KAQK30800-I	Migration terminated. (Policy name: <*policy name*>, Task id: <*task-id*>, Task status: <*task-status*>, Lastexec start time: <*lastexec-start-time*>, Lastexec end time: <*lastexec-end-time*>, Succeeded files: <*succeeded-files*>, Target files: <*target-files*>, Failed files: <*failed-files*>, Post-command result: <*post-command-result*>)	The termination of the migration job occurred.	—		—
KAQK30801-E	MIACAT detected a failure(MAR=<*MAR*> RC=<*RC*>)	A hardware failure occurred in the node and RC is detected.	①	Execute ccp command and acquire the RC information.	"Maintenance Tool '2.61 RC Information Acquisition (ccp)' (MNTT 02-3270)"
			②	Refer to "HitachiAdvancedServer8000/RS220xK [System Unit] Maintenance Manual," and determine the failure part from the RC and the continuous log.	"HitachiAdvancedServer8000/ RS220xK [System Unit] Maintenance Manual"
			③	Replace the part that determined as failed.	"Replacement 'Chapter 1 Replacing the Components of Hitachi Data Ingestor' (REP 01-0000)"
KAQK36504-W	NIC: Link down detected (<*interface-name*>)	NIC became link-down.	Follow the determination flowchart of Troubleshooting 'C.2.3.6 Determination of network failure (3) In the case of the KAQK36504-W'.		'C.2.3.6 Determination of network failure (3) In the case of the KAQK36504-W'

Copyright © 2012, 2016, Hitachi, Ltd.

Message ID	Message text	Description	Recovery method	Reference Page
KAQK36700-E	An FC path error has occurred. (number of LUs for which errors occurred = <*number of LUs for which errors occurred*>)	FC path failure occurred. The number of LUs that the failures are detected is displayed.	Follow the determination flowchart of 'C.2.2 Determination Procedure when a Failure Occurred' and identify the failure location on the FC path.	'C.2.2 Determination Procedure when a Failure Occurred'
KAQK36701-E	Errors have occurred on all the FC paths. (number, subsequent processing of LUs for which errors occurred = <*number, subsequent processing of LUs for which errors occurred*>)	Failures occurred in all paths to the LU. The number of LUs from which failures are detected is displayed. In the case "reboot" is displayed as the subsequent processing, the OS has been restarted once after the failure. In the case "continue" or "failure" is displayed as the subsequent processing, the OS has been running (not restarted). In the case of "disconnect", the OS has been restarted once after the failure usually, but depend on the settings, the OS may have been running without restarting.	Check if the KAQK39527-E message was reported after this message • If it is confirmed, refer to "Message IDs (KAQK39527-E)". • If it is not confirmed, Confirm that the KAQK36700-E message was reported before this message. Perform the same procedure as for "Message IDs (KAQK36700-E)".	'Message IDs (KAQK39527-E)' Message IDs (KAQK36700-E)
KAQK36703-E	An attempt to allocate memory failed.	Failed to allocate memory.	Check if the KAQK36705-E message was reported after this message. • If it is confirmed, refer to "Message IDs (KAQK36705-E)". • If it is not confirmed, follow the determination flowchart of 'C.2.2 Determination Procedure when a Failure Occurred' to identify the failure location on the FC path.	Message IDs (KAQK36705-E) 'C.2.2 Determination Procedure when a Failure Occurred'
KAQK36704-E	An attempt to attach the HDLM driver (the filter component) has failed. Number of failed paths = <number>	Unsupported disk array is detected.	Request the system administrator to check the zoning setting of FC-SW.	—
KAQK36705-E	The system retried to allocate memory but the retries failed.	Memory allocation was attempted in succession but failed.	FC path failure. Follow the determination flowchart of 'C.2.2 Determination Procedure when a Failure Occurred' to identify the failure location on the FC path.	'C.2.2 Determination Procedure when a Failure Occurred'

Copyright © 2012, 2016, Hitachi, Ltd.

Message ID	Message text	Description	Recovery method	Reference Page
KAQK37508-W	BMC network communication failure detected	Communication is lost between the management port and the remote node's BMC port.	Refer to Troubleshooting 'C.2.2 Determination Procedure when a Failure Occurred' to check if this is a management LAN failure.	'C.2.2 Determination Procedure when a Failure Occurred'
KAQK37509-I	BMC network communication failure recovered	Communication is reestablished between the management port and the remote node's BMC port.	—	—
KAQK37510-W	Management network communication failure detected	Communication is lost between the local management port and the remote node's management port.	Refer to Troubleshooting 'C.2.2 Determination Procedure when a Failure Occurred' to check if this is a management LAN failure.	'C.2.2 Determination Procedure when a Failure Occurred'
KAQK37511-I	Management network communication failure recovered	Communication is reestablished between the local management port and the remote node's management port.	—	—
KAQK37512-E	The number of internal RAID device media errors has exceeded the threshold. (internal_disk_<*number*>)	A media error in the built-in HDD is detected.	Replace the built-in HDD that is subject to be replaced for the prevention.	"Replacement '1.3 Replacing the Internal Hard Disk Drive'(REP 01-0110)"
KAQK37513-I	The number of internal RAID device media errors has been cleared. (internal_disk<*number*>)	A media error in the built-in HDD is recovered.	—	—
KAQK37514-E	The number of internal RAID device S.M.A.R.T. warnings has exceeded the threshold. (internal_disk_<*number*>)	The built-in HDD detects S.M.A.R.T. warning.	Replace the built-in HDD that is subject to be replaced for the prevention.	"Replacement '1.3 Replacing the Internal Hard Disk Drive'(REP 01-0110)"
KAQK37515-I	The number of internal RAID device S.M.A.R.T. warnings has been cleared. (internal_disk_<*number*>)	Recovered the S.M.A.R.T. warning that is detected by the built-in HDD.	—	—

Copyright © 2012, 2016, Hitachi, Ltd.

Message ID	Message text	Description	Recovery method	Reference Page
KAQK37516-I	Patrol Read detected information.(Details: time =<*time*>, code = <*code*>, content = <*content*>, count = <*count*>)	Some events about internal HDD were detected. (Number of count is displayed only when the multiple events occurred.)	—	—
KAQK37518-I	Patrol Read detected an error.(Details: time =<*time*>, code = <*code*>, content = <*content*>, count = <*count*>)	Critical Error might be occur at internal HDD. (Number of count is displayed only when the multiple errors occurred.)	The slot number of failed embedded HDD is displayed as "sX (X is positive integer)" in "content" of the message. Replace the embedded HDD connected to that slot number.	"Replacement '1.3 Replacing the Internal Hard Disk Drive'(REP 01-0110)"
KAQK37521-I	Communication temporarily went down between the management port and the BMC port on the other node.	The communication between the management port and the BMC port on the other side node lost temporarily.	Check if KAQK37508-W or KAQK37522-I exists after this SIM. If the message exists, follow the instruction described in that message. If the message does not exist, no measurement is required because the communication was lost temporarily but it recovers at present.	'Message IDs (KAQK37508-W)' Message IDs (KAQK37522-I))
KAQK37522-I	Intermittent failures have been detected <*X*> times between the management port and the BMC port on the other node.	The intermittent failure between the management port and the BMC port in the other side node is detected x times.	Check if KAQK37508-W exists after this SIM. If the message exists, follow the instruction described in that message. If the message does not exist, no measurement is required because the communication was lost temporarily but it recovers at present. However, If this message shows frequency, the cable might not be connected completely. Therefore, check the connection between the cable on the maintenance port and the cable of the BMC port on the other side node.	'Message IDs (KAQK37508-W)'
KAQK37523-I	Information regarding the internal RAID battery was detected. (time = <*time*>, code =0x000c, content = <*content*>)	An event about internal RAID battery was detected.	—	—
KAQK37524-W	An internal RAID battery failure was detected. (time = <*time*>, code = 0x000a, content = <*content*>)	A failure event about internal RAID battery was detected.	There is a possibility that a part of data has been lost. Execute the OS initial installation (with RAID reconfiguration), and request the system administrator to execute the recovery operation. Refer to 'C.1.2 When Detected by SNMP Trap' for more details.	'C.1.2 When Detected by SNMP Trap'
KAQK39500-E	OS error Detail= 00 00 00 01 ,Level =00 , Type=02	The file system necessary for booting is blocked or failed in mounting.	Follow the determination flowchart of 'C.2.2 Determination Procedure when a Failure Occurred'.	'C.2.2 Determination Procedure when a Failure Occurred'
	OS error Detail= 00 00 00 02 ,Level =00 , Type=02	A user file system is blocked.	Follow the determination flowchart of 'C.2.2 Determination Procedure when a Failure Occurred'.	'C.2.2 Determination Procedure when a Failure Occurred'
	OS error Detail= 00 00 00 02 ,Level =00 , Type=0c	The logical volume entered a state where it cannot be accessed. (The file system or differential-data snapshots can no longer be used.)	Ask the system administrator to confirm whether KAQG51003-E message has been output at the system message. If the message has been output, confirm to system administrator that an appropriate action about KAQG51003-E has been finished. And acquire the trouble information and send it to the Technical Support Center. If the message has not been output, acquires the trouble information and send it to the Technical Support Center with the comment that "There has not been output KAQG51003-E".	"Troubleshooting 'Chapter 6 Acquiring Failure Information' (TRBL 06-0000)"

Copyright © 2012, 2016, Hitachi, Ltd.

Message ID	Message text	Description	Recovery method		Reference Page
(Continued) KAQK39500-E	OS error Detail= 00 00 00 03 ,Level =00 , Type=02	A cluster management LU file system is blocked.	Follow the determination flowchart of Troubleshooting “9.1.3 Recovery Procedure for Software Failure”.		“Troubleshooting ‘9.1.3 Recovery Procedure for Software Failure’ (TRBL 09-0050)”
	OS error Detail= 00 00 00 06 ,Level =00 , Type=02	A Virtual Server system LU is blocked.	Follow the determination flowchart of Troubleshooting “9.1.3 Recovery Procedure for Software Failure”.		“Troubleshooting ‘9.1.3 Recovery Procedure for Software Failure’ (TRBL 09-0050)”
	OS error Detail= 00 00 03 00 ,Level =00 , Type=0D	Breakdown of the heartbeat between the primary and the secondary is detected.	①	Perform “clstatus” on the node that have this SIM message, and check the cluster status.	“Maintenance Tool ‘2.2 Displaying the Cluster Status (clstatus)’ (MNTT 02-0040)”
			②	‘C.2.2 Determination Procedure when a Failure Occurred’	‘C.2.2 Determination Procedure when a Failure Occurred’
	OS error Detail= 00 00 03 01 ,Level =00 , Type=0D	Breakdown of the heartbeats between the primary and the secondary is detected, and resetting route on the management LAN is detected.	To confirm the failure on the management LAN, execute the determination procedure from the ‘C.2.2 Determination Procedure when a Failure Occurred’.		‘C.2.2 Determination Procedure when a Failure Occurred’
	OS error Detail= 00 00 04 00 ,Level =00 , Type=0D	The reset ping-pong prevention was operated.	Follow the determination flowchart of ‘C.2.2 Determination Procedure when a Failure Occurred’.		‘C.2.2 Determination Procedure when a Failure Occurred’
	OS error Detail= 00 01 00 02 ,Level =00 , Type=0A	The target file system to be stored is initialized before creating dump file.	Node is rebooted because of occurrence of an error, and an error is detected while collecting Dump. Collect the information of troubles, and report it to the Technical Support Center after executing troubleshooting with referring to the chapter of troubleshooting.		“Troubleshooting ‘Chapter 6 Acquiring Failure Information’ (TRBL 06-0000)”
	OS error Detail= 00 02 00 02 ,Level =00 , Type=0A	Failed to mount the target file system to be stored at the time of dump collecting.	An error detected in the dump area while starting the node. Execute troubleshooting with referring to ‘C.2.2 Determination Procedure when a Failure Occurred’.		‘C.2.2 Determination Procedure when a Failure Occurred’
	OS error Detail= 05 00 00 00 ,Level =00 , Type=03	A panic failure occurred on the node that failed.	①	• If it is after nncreset command execution of the “Maintenance Tool ‘2.30 Resetting the OS of the Node (nncreset)’” performed by the maintenance personnel, proceed to step②. • If it is not a result of the command that is executed by the maintenance personnel, proceed to step③.	“Maintenance Tool ‘2.30 Resetting the OS of the Node (nncreset)’ (MNTT 02-1840)”
			②	It indicates that the nncreset command successfully complete and the dump can be obtained normally. Proceed to the next step such as the collecting dump.	—
			③	A panic failure occurred on the node that failed, and the dump can be obtained normally after the failure. Refer to ‘C.2.3.4 Determining the node failure when failover occurred,’ and then execute the failure determination.	‘C.2.3.4 Determining the node failure when failover occurred’

Copyright © 2012, 2016, Hitachi, Ltd.

Message ID	Message text	Description	Recovery method		Reference Page
(Continued) KAQK39500-E	OS error Detail= 05 00 00 01 ,Level =00 , Type=03	Memory image copying is complete successfully.	①	• If it is manual dump collection by the system administrator or the maintenance personnel (dump collection by the NMI button or the nncreset command of "Maintenance Tool '2.30 Resetting the OS of the Node (nncreset)'", proceed to step②. • In other cases than the above, proceed to step③.	"Maintenance Tool '2.30 Resetting the OS of the Node (nncreset)' (MNTT 02-1840)"
			②	After a while, if "KAQK39528-I Processing to convert dump files ended." is displayed, as the dump file conversion is successful, execute the subsequent operation such as downloading dump. If the other SIM than the above is displayed after a while, the dump file creation failed. Collect the failure information, and contact the developer.	"Troubleshooting 'Chapter 6 Acquiring Failure Information' (TRBL 06-0000)'
			③	A panic failure occurred on the failed node, and then the dump is acquired normally. Refer to 'C.2.3.4 Determining the node failure when failover occurred', and determine the failure.	'C.2.3.4 Determining the node failure when failover occurred'
	OS error Detail= 06 00 00 00 ,Level =00 , Type=03	Dump conversion timeout.	The node is rebooted due to a software failure. Collect the failure information and contact the developer.		"Troubleshooting 'Chapter 6 Acquiring Failure Information' (TRBL 06-0000)"
	OS error Detail= 06 00 01 00 ,Level =00 , Type=03	Dump file conversion failed.	The node is rebooted due to a software failure. Collect the failure information and contact the developer.		"Troubleshooting 'Chapter 6 Acquiring Failure Information' (TRBL 06-0000)"
	OS error Detail= 06 00 02 00 ,Level =00 , Type=03	Forced conversion of the dump file failed.	The node is rebooted due to a software failure. Collect the failure information and contact the developer.		"Troubleshooting 'Chapter 6 Acquiring Failure Information' (TRBL 06-0000)"
	OS error Detail= 06 00 03 00 ,Level =00 , Type=03	Memory image copying failed.	The node is rebooted due to a software failure. Collect the failure information and contact the developer.		"Troubleshooting 'Chapter 6 Acquiring Failure Information' (TRBL 06-0000)"
	OS error Detail= 06 01 01 00 ,Level =00 , Type=0A	Failed to register the function of dump file creation.	Failed to register the dump file creation function which is executed at the time of boot the node. Collect the failure information and contact the developer.		"Troubleshooting 'Chapter 6 Acquiring Failure Information' (TRBL 06-0000)"
KAQK39501-E	Fatal failure detected. Shutting down.	An emergency shutdown occurred.	—		—
KAQK39502-I	OS is ready	This message is reported just before completion of the OS boot.	—		—
KAQK39503-I	OS is shutting down.	This message reports that shutdown of either system or both systems have started.	—		—
KAQK39504-E	Link down in Front-end LAN	The data LAN or the maintenance LAN is link-down.	Follow the determination flowchart of Troubleshooting 'C.2.3.6 Determination of network failure (4) In the case of the KAQK39504-E'.		'C.2.3.6 Determination of network failure (4) In the case of the KAQK39504-E'

Copyright © 2011, 2016, Hitachi, Ltd.

Message ID	Message text	Description	Recovery method	Reference Page
KAQK39505-E	OS error[cluster] Detail= 00 01 00 00	Mounting the cluster management LU failed (CLU_partition failure).	Refer to the failure recovery procedure of Troubleshooting “Chapter 9 Confirmation of Hardware Failure Recovery and Recovery Procedure for Software Failure” and recover the failure.	“Troubleshooting ‘Chapter 9 Confirmation of Hardware Failure Recovery and Recovery Procedure for Software Failure’ (TRBL 09-0000)”
	OS error[cluster] Detail=00 02 00 00	Pre-processing of NFS failed.	Refer to the failure recovery procedure of Troubleshooting “Chapter 9 Confirmation of Hardware Failure Recovery and Recovery Procedure for Software Failure” and recover the failure.	“Troubleshooting ‘Chapter 9 Confirmation of Hardware Failure Recovery and Recovery Procedure for Software Failure’ (TRBL 09-0000)”
	OS error[cluster] Detail=00 03 00 00	Mounting the file system failed.	Ask the system administrator for the enabling or disabling of the local data encryption and the HCP payload encryption.. If the local data encryption is enabled, ask the system administrator to confirm one of the system messages KAQM05256-E, KAQM05258-E to KAQM05264-E, KAQM05323-E, KAQM05325-W has not been output. In case the one of the messages has been output, ask the system administrator to take an appropriate action. If no message has been output, or the local data encryption and HCP payload encryption are disabled, refer to the failure recovery procedure of Troubleshooting “Chapter 9 Confirmation of Hardware Failure Recovery and Recovery Procedure for Software Failure” and recover the failure.	“Troubleshooting ‘Chapter 9 Confirmation of Hardware Failure Recovery and Recovery Procedure for Software Failure’ (TRBL 09-0000)”
	OS error[cluster] Detail= 00 04 00 00	Starting the NFS sharing failed.	Refer to the failure recovery procedure of Troubleshooting “Chapter 9 Confirmation of Hardware Failure Recovery and Recovery Procedure for Software Failure” and recover the failure.	“Troubleshooting ‘Chapter 9 Confirmation of Hardware Failure Recovery and Recovery Procedure for Software Failure’ (TRBL 09-0000)”

Copyright © 2011, 2016, Hitachi, Ltd.

Message ID	Message text	Description	Recovery method	Reference Page
(Continued) KAQK39505-E	OS error[cluster] Detail= 00 05 00 00	Bringing the virtual IP up failed.	① Check if the KAQK39504-E message was reported within 60 seconds before or after this message. • If it is confirmed, proceed to step②. • If it is not confirmed, proceed to step③.	'Message IDs (KAQK39504-E)'
			② Perform the maintenance procedure described in "Message IDs (KAQK39504-E)".	'Message IDs (KAQK39504-E)'
			③ Refer to the failure recovery procedure of Troubleshooting "Chapter 9 Confirmation of Hardware Failure Recovery and Recovery Procedure for Software Failure" and recover the failure.	"Troubleshooting 'Chapter 9 Confirmation of Hardware Failure Recovery and Recovery Procedure for Software Failure' (TRBL 09-0000)"
	OS error[cluster] Detail= 00 06 00 00	Starting the CIFS service failed.	Refer to the failure recovery procedure of Troubleshooting "Chapter 9 Confirmation of Hardware Failure Recovery and Recovery Procedure for Software Failure" and recover the failure.	"Troubleshooting 'Chapter 9 Confirmation of Hardware Failure Recovery and Recovery Procedure for Software Failure' (TRBL 09-0000)"
	OS error[cluster] Detail= 00 08 00 00	Startup processing of the resource group failed.	Refer to the failure recovery procedure of Troubleshooting "Chapter 9 Confirmation of Hardware Failure Recovery and Recovery Procedure for Software Failure" and recover the failure.	"Troubleshooting 'Chapter 9 Confirmation of Hardware Failure Recovery and Recovery Procedure for Software Failure' (TRBL 09-0000)"
	OS error[cluster] Detail= 00 0A 00 00	File snapshot or file version restore function failure (Startup processing of the resource group failed.)	Refer to the failure recovery procedure of Troubleshooting "Chapter 9 Confirmation of Hardware Failure Recovery and Recovery Procedure for Software Failure" and recover the failure.	"Troubleshooting 'Chapter 9 Confirmation of Hardware Failure Recovery and Recovery Procedure for Software Failure' (TRBL 09-0000)"
	OS error[cluster] Detail= 00 0B 00 00	Start processing of Virtual Server failed.	Ask the system administrator for the enabling or disabling of the local data encryption and the HCP payload encryption.. If the local data encryption is enabled, ask the system administrator to confirm one of the system messages KAQM05256-E, KAQM05258-E to KAQM05264-E, KAQM05323-E, KAQM05325-W has not been output. In case the one of the messages has been output, ask the system administrator to take an appropriate action. If no message has been output, or the local data encryption and HCP payload encryption are disabled, refer to the failure recovery procedure of Troubleshooting "Chapter 9 Confirmation of Hardware Failure Recovery and Recovery Procedure for Software Failure" and recover the failure.	"Troubleshooting 'Chapter 9 Confirmation of Hardware Failure Recovery and Recovery Procedure for Software Failure' (TRBL 09-0000)"

Copyright © 2012, 2016, Hitachi, Ltd.

Message ID	Message text	Description	Recovery method	Reference Page
(Continued) KAQK39505-E	OS error[cluster] Detail=01 01 00 00	Un mounting the cluster management LU failed (CLU_partition failure).	Refer to the failure recovery procedure of Troubleshooting “Chapter 9 Confirmation of Hardware Failure Recovery and Recovery Procedure for Software Failure” and recover the failure.	“Troubleshooting ‘Chapter 9 Confirmation of Hardware Failure Recovery and Recovery Procedure for Software Failure’ (TRBL 09-0000)”
	OS error[cluster] Detail=01 02 00 00	Post-processing of NFS failed.	Refer to the failure recovery procedure of Troubleshooting “Chapter 9 Confirmation of Hardware Failure Recovery and Recovery Procedure for Software Failure” and recover the failure.	“Troubleshooting ‘Chapter 9 Confirmation of Hardware Failure Recovery and Recovery Procedure for Software Failure’ (TRBL 09-0000)”
	OS error[cluster] Detail=01 03 00 00	Unmounting the file system failed.	Refer to the failure recovery procedure of Troubleshooting “Chapter 9 Confirmation of Hardware Failure Recovery and Recovery Procedure for Software Failure” and recover the failure.	“Troubleshooting ‘Chapter 9 Confirmation of Hardware Failure Recovery and Recovery Procedure for Software Failure’ (TRBL 09-0000)”
	OS error[cluster] Detail= 01 04 00 00	Stopping the NFS sharing failed.	Refer to the failure recovery procedure of Troubleshooting “Chapter 9 Confirmation of Hardware Failure Recovery and Recovery Procedure for Software Failure” and recover the failure.	“Troubleshooting ‘Chapter 9 Confirmation of Hardware Failure Recovery and Recovery Procedure for Software Failure’ (TRBL 09-0000)”
	OS error[cluster] Detail= 01 05 00 00	Bringing the virtual IP down failed.	① Check if the KAQK39504-E message was reported within 60 seconds before or after this message. • If it is confirmed, proceed to step②. • If it is not confirmed, proceed to step③.	‘Message IDs (KAQK39504-E)’
			② Perform the maintenance procedure described in “Message IDs (KAQK39504-E)”.	‘Message IDs (KAQK39504-E)’
			③ Refer to the failure recovery procedure of Troubleshooting “Chapter 9 Confirmation of Hardware Failure Recovery and Recovery Procedure for Software Failure” and recover the failure.	“Troubleshooting ‘Chapter 9 Confirmation of Hardware Failure Recovery and Recovery Procedure for Software Failure’ (TRBL 09-0000)”

Copyright © 2012, 2016, Hitachi, Ltd.

Message ID	Message text	Description	Recovery method	Reference Page
(Continued) KAQK39505-E	OS error[cluster] Detail= 01 06 00 00	Stopping the CIFS service failed.	Refer to the failure recovery procedure of Troubleshooting “Chapter 9 Confirmation of Hardware Failure Recovery and Recovery Procedure for Software Failure” and recover the failure.	“Troubleshooting ‘Chapter 9 Confirmation of Hardware Failure Recovery and Recovery Procedure for Software Failure’ (TRBL 09-0000)”
	OS error[cluster] Detail= 01 08 00 00	Stop processing of the resource group failed.	Refer to the failure recovery procedure of Troubleshooting “Chapter 9 Confirmation of Hardware Failure Recovery and Recovery Procedure for Software Failure” and recover the failure.	“Troubleshooting ‘Chapter 9 Confirmation of Hardware Failure Recovery and Recovery Procedure for Software Failure’ (TRBL 09-0000)”
	OS error[cluster] Detail= 01 0A 00 00	File snapshot or file version restore function failure (Stop processing of the resource group failed.)	Refer to the failure recovery procedure of Troubleshooting “Chapter 9 Confirmation of Hardware Failure Recovery and Recovery Procedure for Software Failure” and recover the failure.	“Troubleshooting ‘Chapter 9 Confirmation of Hardware Failure Recovery and Recovery Procedure for Software Failure’ (TRBL 09-0000)”
	OS error[cluster] Detail= 01 0B 00 00	Stopping Virtual Server failed	Refer to the failure recovery procedure of Troubleshooting “Chapter 9 Confirmation of Hardware Failure Recovery and Recovery Procedure for Software Failure” and recover the failure.	“Troubleshooting ‘Chapter 9 Confirmation of Hardware Failure Recovery and Recovery Procedure for Software Failure’ (TRBL 09-0000)”

Copyright © 2013, 2016, Hitachi, Ltd.

Message ID	Message text	Description	Recovery method	Reference Page
KAQK39506-I	A failure occurred. Please follow the proper recovery procedure. Detail=10 03 00 00	All file systems were blocked due to D-vol overflow (when the script was started).	Send the content of this message to the system administrator.	—
	A failure occurred. Please follow the proper recovery procedure. Detail=10 04 00 00	All NFSs were blocked due to D-vol overflow (when the script was started).	Send the content of this message to the system administrator.	—
KAQK39507-E	Reset to the other node in the cluster was requested (result:<*reset requested result*>, cause:<*reset cause*>, os status:<*OS status*>).	Resetting for the other side is issued.	If the content of the result is "failure", resetting the other side node is not successful. Determine the failure with 'C.2.2 Determination Procedure when a Failure Occurred'. If the content of the result is other than above, it is normal processing and not required any troubleshooting.	'C.2.2 Determination Procedure when a Failure Occurred'
KAQK39524-E	Peer os status could not be acquired.	Acquisition of status of the other side node failed.	① Check if the KAQK37508-W message was reported before or after reporting the KAQK39508-E message. • If it is reported, refer to "Message IDs (KAQK37508-W)". • If it is not reported, proceed to step②.	'Message IDs (KAQK37508-W)'
			② A failure is in the setting of BMC. Refer to "Maintenance tool 2.18 Setting BMC LAN Information (bmcctl) (3) Setting BMC account", and then set the BMC account.	"Maintenance Tool '2.18 Setting BMC LAN Information (bmcctl)' (MNTT 02-1210)"
KAQK39525-I	Peer os status could be acquired.	Recovered to the state to get the other side node status.	—	—
KAQK39526-I	The blockage of the file system (file-system-name) has been released.	The blockage of the file system (file-system name) has been released.	—	—
KAQK39527-E	A file system (file system name = <*file system name*>, device = <*device number*>) is blocked because there is no unused capacity in the Pool	The user file system has been in blockage because of the DP pool exhaustion.	Ask system administrator to recover the DP pool exhaustion.	—
KAQK39528-I	Processing to convert dump files ended.	Dump file conversion ended normally.	—	—
KAQK39529-E	Dump file conversion processing for the virtual server ended successfully. (virtual server ID = <*virtual server ID*>)	Dump file conversion of the displayed Virtual Server ID ended normally	After a while, if the message of "KAQK39539-I Conversion processing ended successfully for all the dump files." is displayed on the window, the dump file conversion for all the Virtual Servers is successfully complete. Therefore, proceed to the next step such as the dump collection.	—

Copyright © 2012, 2017, Hitachi, Ltd.

Message ID	Message text	Description	Recovery method	Reference Page
KAQK39530-E	Acquisition of the dump file header information for the virtual server failed. (virtual server ID = <*virtual server ID*>)	Failed to get the dump file header information of the displayed Virtual Server ID.	Request the system administrator to reboot the relevant Virtual Server of the ID that is displayed on the window. When the system administrator is not available to operate it, maintenance personnel should execute this process by using vnasrestart command. If the same SIM message is displayed after the reboot, collect the failure information and contact the Technical Support Center.	"Maintenance Tool '2.77 Restart of Virtual Server (vnasrestart)' (MNTT 02-4090) "Troubleshooting 'Chapter 6 Acquiring Failure Information' (TRBL 06-0000)"
KAQK39531-E	Dump file creation processing failed because the number of virtual server dump files reached the limit. (virtual server ID = <*virtual server ID*>)	The dump file of the displayed Virtual Server ID could not be created because the number of dump files has reached 5 files that was the upper limit of file storage.	Collect the failure information, and contact the Technical Support Center. The dump file of the displayed Virtual Server ID is not created even after some existing dump files are deleted. If the dump file of the displayed Virtual Server ID is necessary, refer to Troubleshooting "6.2.1.2 Collecting dump files manually", and then collect the dump file.	"Troubleshooting 'Chapter 6 Acquiring Failure Information' (TRBL 06-0000)" "Troubleshooting '6.2.1.2 Collecting dump files manually' (TRBL 06-0030)"
KAQK39532-E	Dump file creation processing failed. (virtual server ID = <*virtual server ID*>)	Failed to create the dump file of the displayed Virtual Server ID because the capacity of the dump file storage area was insufficient.	Collect the failure information, and contact the Technical Support Center. The dump file of the displayed Virtual Server ID is not created even after some existing dump files are deleted. If the dump file of the displayed Virtual Server ID is necessary, refer to Troubleshooting "6.2.1.2 Collecting dump files manually", and then collect the dump file.	"Troubleshooting 'Chapter 6 Acquiring Failure Information' (TRBL 06-0000)" "Troubleshooting '6.2.1.2 Collecting dump files manually' (TRBL 06-0030)"
KAQK39533-E	Dump file conversion processing for the virtual server was stopped.	Dump file conversion processing was inhibited because the capacity of dump file storage area was insufficient.	Download all the stored dump files and delete them all. After that, the converting process of the unconverted dump files is executed automatically.	"Maintenance Tool '2.21 Procedure for Collecting Dump Files' (MNTT 02-1400)
KAQK39534-E	Dump file forced conversion processing for the virtual server ended successfully. (virtual server ID = <*virtual server ID*>)	Although the dump file conversion processing of the displayed Virtual Server ID is complete, a problem might have occurred on a part of converting process.	Collect the failure information, and then contact the technical support center.	"Troubleshooting 'Chapter 6 Acquiring Failure Information' (TRBL 06-0000)"
KAQK39535-E	Dump file conversion processing for the virtual server failed.(virtual server ID = <*virtual server ID*>)	Failed the convert the dump file of displayed Virtual Server ID.	Collect the failure information, and then contact the technical support center.	"Troubleshooting 'Chapter 6 Acquiring Failure Information' (TRBL 06-0000)"
KAQK39536-E	An error occurred in dump file creation processing for the virtual server.	Failed to create the dump file of displayed Virtual Server ID.	Collect the failure information, and then contact the technical support center.	"Troubleshooting 'Chapter 6 Acquiring Failure Information' (TRBL 06-0000)"

Copyright © 2011, 2016, Hitachi, Ltd.

Message ID	Message text	Description	Recovery method	Reference Page
KAQK39538-E	An OS error was detected on the virtual server.(virtual server ID = <virtual server ID>)	The virtual Server of the displayed Virtual Server ID is blocked.	Execute the troubleshooting from the 'C.2.2 Determination Procedure when a Failure Occurred'.	'C.2.2 Determination Procedure when a Failure Occurred'
KAQK39539-I	Conversion processing ended successfully for all the dump files.	Converting all the unconverted dump files is complete.	—	—
KAQK39540-I	The virtual server was reset. (virtual server ID=<virtual server ID>)	The displayed Virtual Server ID was reset.	—	—
KAQK39601-E	Single Node error Detail=00 00 00 10 Level=00 Type=04	Mounting of file system failed.	Ask the system administrator for the enabling or disabling of the local data encryption and the HCP payload encryption.. If the local data encryption is enabled, ask the system administrator to confirm one of the system messages KAQM05256-E, KAQM05258-E to KAQM05264-E, KAQM05323-E, KAQM05325-W has not been output. In case the one of the messages has been output, ask the system administrator to take an appropriate action. If no message has been output, or the local data encryption and HCP payload encryption are disabled, refer to the failure recovery procedure of Troubleshooting "Chapter 9 Confirmation of Hardware Failure Recovery and Recovery Procedure for Software Failure" and recover the failure.	"Troubleshooting 'Chapter 9 Confirmation of Hardware Failure Recovery and Recovery Procedure for Software Failure' (TRBL 09-0000)"
	Single Node error Detail=00 00 00 11 Level=00 Type=04	Dismounting of file system failed.	Refer to the failure recovery procedure of Troubleshooting "Chapter 9 Confirmation of Hardware Failure Recovery and Recovery Procedure for Software Failure" and recover the failure.	"Troubleshooting 'Chapter 9 Confirmation of Hardware Failure Recovery and Recovery Procedure for Software Failure' (TRBL 09-0000)"
	Single Node error Detail=00 00 00 20 Level=00 Type=04	Starting the NFS sharing failed.	Refer to the failure recovery procedure of Troubleshooting "Chapter 9 Confirmation of Hardware Failure Recovery and Recovery Procedure for Software Failure" and recover the failure.	"Troubleshooting 'Chapter 9 Confirmation of Hardware Failure Recovery and Recovery Procedure for Software Failure' (TRBL 09-0000)"
	Single Node error Detail=00 00 00 21 Level=00 Type=04	Terminating the NFS sharing failed.	Refer to the failure recovery procedure of Troubleshooting "Chapter 9 Confirmation of Hardware Failure Recovery and Recovery Procedure for Software Failure" and recover the failure.	"Troubleshooting 'Chapter 9 Confirmation of Hardware Failure Recovery and Recovery Procedure for Software Failure' (TRBL 09-0000)"
	Single Node error Detail=00 00 00 40 Level=00 Type=04	Startup of the CIFS service failed.	Refer to the failure recovery procedure of Troubleshooting "Chapter 9 Confirmation of Hardware Failure Recovery and Recovery Procedure for Software Failure" and recover the failure.	"Troubleshooting 'Chapter 9 Confirmation of Hardware Failure Recovery and Recovery Procedure for Software Failure' (TRBL 09-0000)"

Copyright © 2012, 2016, Hitachi, Ltd.

Message ID	Message text	Description	Recovery method	Reference Page
(Continued) KAQK39601-E	Single Node error Detail=00 00 00 41 Level=00 Type=04	Stopping of the CIFS service failed.	Refer to the failure recovery procedure of Troubleshooting “Chapter 9 Confirmation of Hardware Failure Recovery and Recovery Procedure for Software Failure” and recover the failure.	“Troubleshooting ‘Chapter 9 Confirmation of Hardware Failure Recovery and Recovery Procedure for Software Failure’ (TRBL 09-0000)”
	Single Node error Detail=00 00 00 50 Level=00 Type=04	Startup of the File snapshot or the file version restore function failed.	Refer to the failure recovery procedure of Troubleshooting “Chapter 9 Confirmation of Hardware Failure Recovery and Recovery Procedure for Software Failure” and recover the failure.	“Troubleshooting ‘Chapter 9 Confirmation of Hardware Failure Recovery and Recovery Procedure for Software Failure’ (TRBL 09-0000)”
	Single Node error Detail=00 00 00 51 Level=00 Type=04	Stopping of the File snapshot or the file version restore function failed.	Refer to the failure recovery procedure of Troubleshooting “Chapter 9 Confirmation of Hardware Failure Recovery and Recovery Procedure for Software Failure” and recover the failure.	“Troubleshooting ‘Chapter 9 Confirmation of Hardware Failure Recovery and Recovery Procedure for Software Failure’ (TRBL 09-0000)”
	Single Node error Detail=00 00 00 F0 Level=00 Type=04	Startup of the resource on the single node failed.	Refer to the failure recovery procedure of Troubleshooting “Chapter 9 Confirmation of Hardware Failure Recovery and Recovery Procedure for Software Failure” and recover the failure.	“Troubleshooting ‘Chapter 9 Confirmation of Hardware Failure Recovery and Recovery Procedure for Software Failure’ (TRBL 09-0000)”
	Single Node error Detail=00 00 00 F1 Level=00 Type=04	Stopping of the resource on the single node failed.	Refer to the failure recovery procedure of Troubleshooting “Chapter 9 Confirmation of Hardware Failure Recovery and Recovery Procedure for Software Failure” and recover the failure.	“Troubleshooting ‘Chapter 9 Confirmation of Hardware Failure Recovery and Recovery Procedure for Software Failure’ (TRBL 09-0000)”

Copyright © 2012, 2016, Hitachi, Ltd.

Message ID	Message text	Description	Recovery method	Reference Page
KAQK39602-E	Virtual Server error Detail=00 00 01 10 Level=00 Type=04	Failed to mount the file system of the displayed Virtual Server ID.	Ask the system administrator for the enabling or disabling of the local data encryption and the HCP payload encryption.. If the local data encryption is enabled, ask the system administrator to confirm one of the system messages KAQM05256-E, KAQM05258-E to KAQM05264-E, KAQM05323-E, KAQM05325-W has not been output. In case the one of the messages has been output, ask the system administrator to take an appropriate action. If no message has been output, or the local data encryption and HCP payload encryption are disabled, refer to the failure recovery procedure of Troubleshooting “Chapter 9 Confirmation of Hardware Failure Recovery and Recovery Procedure for Software Failure” and recover the failure.	“Troubleshooting ‘Chapter 9 Confirmation of Hardware Failure Recovery and Recovery Procedure for Software Failure’ (TRBL 09-0000)”
	Virtual Server error Detail=00 00 01 11 Level=00 Type=04	Failed to unmount (umount) the file system of the displayed Virtual Server ID.	Refer to the failure recovery procedure of Troubleshooting “Chapter 9 Confirmation of Hardware Failure Recovery and Recovery Procedure for Software Failure” and recover the failure.	“Troubleshooting ‘Chapter 9 Confirmation of Hardware Failure Recovery and Recovery Procedure for Software Failure’ (TRBL 09-0000)”
	Virtual Server error Detail=00 00 01 20 Level=00 Type=04	Failed to start the NFS sharing of the displayed Virtual Server ID.	Refer to the failure recovery procedure of Troubleshooting “Chapter 9 Confirmation of Hardware Failure Recovery and Recovery Procedure for Software Failure” and recover the failure.	“Troubleshooting ‘Chapter 9 Confirmation of Hardware Failure Recovery and Recovery Procedure for Software Failure’ (TRBL 09-0000)”
	Virtual Server error Detail=00 00 01 21 Level=00 Type=04	Failed to terminate the NFS sharing of the displayed Virtual Server ID.	Refer to the failure recovery procedure of Troubleshooting “Chapter 9 Confirmation of Hardware Failure Recovery and Recovery Procedure for Software Failure” and recover the failure.	“Troubleshooting ‘Chapter 9 Confirmation of Hardware Failure Recovery and Recovery Procedure for Software Failure’ (TRBL 09-0000)”
	Virtual Server error Detail=00 00 01 30 Level=00 Type=04	Failed to make up the virtual IP of the displayed Virtual Server ID.	Refer to the failure recovery procedure of Troubleshooting “Chapter 9 Confirmation of Hardware Failure Recovery and Recovery Procedure for Software Failure” and recover the failure.	“Troubleshooting ‘Chapter 9 Confirmation of Hardware Failure Recovery and Recovery Procedure for Software Failure’ (TRBL 09-0000)”
	Virtual Server error Detail=00 00 01 31 Level=00 Type=04	Failed to make down the virtual IP of the displayed Virtual Server ID.	Refer to the failure recovery procedure of Troubleshooting “Chapter 9 Confirmation of Hardware Failure Recovery and Recovery Procedure for Software Failure” and recover the failure.	“Troubleshooting ‘Chapter 9 Confirmation of Hardware Failure Recovery and Recovery Procedure for Software Failure’ (TRBL 09-0000)”

Copyright © 2012, 2016, Hitachi, Ltd.

Message ID	Message text	Description	Recovery method	Reference Page
(Continued) KAQK39602-E	Virtual Server error Detail=00 00 01 40 Level=00 Type=04	Failed to start the CIFS service of the displayed Virtual Server ID.	Refer to the failure recovery procedure of Troubleshooting “Chapter 9 Confirmation of Hardware Failure Recovery and Recovery Procedure for Software Failure” and recover the failure.	“Troubleshooting ‘Chapter 9 Confirmation of Hardware Failure Recovery and Recovery Procedure for Software Failure’ (TRBL 09-0000)”
	Virtual Server error Detail=00 00 01 41 Level=00 Type=04	Failed to stop the CIFS service of the displayed Virtual Server ID.	Refer to the failure recovery procedure of Troubleshooting “Chapter 9 Confirmation of Hardware Failure Recovery and Recovery Procedure for Software Failure” and recover the failure.	“Troubleshooting ‘Chapter 9 Confirmation of Hardware Failure Recovery and Recovery Procedure for Software Failure’ (TRBL 09-0000)”
	Virtual Server error Detail=00 00 01 50 Level=00 Type=04	Failed to start the File snapshot of the displayed Virtual Server ID or the file version restore function.	Refer to the failure recovery procedure of Troubleshooting “Chapter 9 Confirmation of Hardware Failure Recovery and Recovery Procedure for Software Failure” and recover the failure.	“Troubleshooting ‘Chapter 9 Confirmation of Hardware Failure Recovery and Recovery Procedure for Software Failure’ (TRBL 09-0000)”
	Virtual Server error Detail=00 00 01 51 Level=00 Type=04	Failed to stop the File snapshot of the displayed Virtual Server ID or the file version restore function.	Refer to the failure recovery procedure of Troubleshooting “Chapter 9 Confirmation of Hardware Failure Recovery and Recovery Procedure for Software Failure” and recover the failure.	“Troubleshooting ‘Chapter 9 Confirmation of Hardware Failure Recovery and Recovery Procedure for Software Failure’ (TRBL 09-0000)”
	Virtual Server error Detail=00 00 01 F0 Level=00 Type=04	Failed to start the Virtual Server resources of the displayed Virtual Server ID.	Refer to the failure recovery procedure of Troubleshooting “Chapter 9 Confirmation of Hardware Failure Recovery and Recovery Procedure for Software Failure” and recover the failure.	“Troubleshooting ‘Chapter 9 Confirmation of Hardware Failure Recovery and Recovery Procedure for Software Failure’ (TRBL 09-0000)”
	Virtual Server error Detail= 00 00 01 F1 Level=00 Type=04	Failed to stop the Virtual Server resources of the displayed Virtual Server ID.	Refer to the failure recovery procedure of Troubleshooting “Chapter 9 Confirmation of Hardware Failure Recovery and Recovery Procedure for Software Failure” and recover the failure.	“Troubleshooting ‘Chapter 9 Confirmation of Hardware Failure Recovery and Recovery Procedure for Software Failure’ (TRBL 09-0000)”

Copyright © 2012, 2016, Hitachi, Ltd.

Message ID	Message text	Description	Recovery method		Reference Page
KAQK39603-E	An attempt to connect user disk failed. (Detail=00 00 02 01 Level=00 Type=04)	Initialization process of the user disk failed.	Refer to the failure recovery procedure of Troubleshooting “9.2.3.1.3 Failure recovery of the blocked file system in the configuration connected to the disk array subsystem” and recover the failure.		“Troubleshooting ‘9.2.3.1.3 Failure recovery of the blocked file system in the configuration connected to the disk array subsystem’ (TRBL 09-0672)”
	An attempt to connect user disk failed. (Detail=00 00 02 02 Level=00 Type=04)	The configuration of user disk is invalid.	①	Execute fpstatus command, and reboot the OS if “Status” of all paths are “Online”. If any “Status” other than “Online” is included, proceed to step②.	“Maintenance Tool ‘2.5 Displaying the FC Status (fpstatus)’ (MNTT 02-0280)” “Maintenance Tool ‘2.29 Rebooting the OS of This Side Node (nasreboot)’ (MNTT 02-1790)”
			②	Refer to the failure recovery procedure of Troubleshooting “5.1 Determining FC Path Failures” and recover the failure.	“Troubleshooting ‘5.1 Determining FC Path Failures’ (TRBL 05-0000)”

Copyright © 2012, 2016, Hitachi, Ltd.

C.3.2 LCD Display Message Code

This is unsupported configuration in this mode.

Copyright © 2011, 2013, Hitachi, Ltd.

C.3.3 KAQX Messages

This model does not support relations with HCP Anywhere.

Copyright © 2015, Hitachi, Ltd.

This page is for editorial purpose only.

Copyright © 2015, Hitachi, Ltd.

CONTENTS

D.1 Replacing the Components

D.1.1 Replacing the Power Supply Unit/ AC Cable

D.1.1.1 Replacing the Power Supply Unit/ AC Cable (cluster configuration)

D.1.1.2 Replacing the Power Supply Unit/ AC Cable (single node configuration)

D.1.2 Replacing the Fan Unit

D.1.2.1 Replacing the Fan Unit (cluster configuration)

D.1.2.2 Replacing the Fan Unit (single node configuration)

D.1.3 Replacing the Internal Hard Disk Drive

D.1.3.1 Replacing the Internal Hard Disk Drive (cluster configuration)

D.1.3.2 Replacing the Internal Hard Disk Drive (single node configuration)

D.1.4 Replacing the RAID Controller

D.1.4.1 Replacing the RAID Controller (cluster configuration)

D.1.4.2 Replacing the RAID Controller (single node configuration)

D.1.5 Replacing the Memory

D.1.5.1 Replacing the Memory (cluster configuration)

D.1.5.2 Replacing the Memory (single node configuration)

D.1.6 Replacing the Fibre Channel Card

D.1.6.1 Replacing the Fibre Channel Card (cluster configuration)

D.1.6.2 Replacing the Fibre Channel Card (single node configuration)

D.1.7 Replacing the GbE-4Port Card

D.1.7.1 Replacing the GbE-4Port Card (cluster configuration)

D.1.7.2 Replacing the GbE-4Port Card (single node configuration)

D.1.8 Replacing the GbE-2Port Card

D.1.8.1 Replacing the GbE-2Port Card (cluster configuration)

D.1.8.2 Replacing the GbE-2Port Card (single node configuration)

D.1.9 Replacing the Motherboard

D.1.9.1 Replacing the Motherboard (cluster configuration)

D.1.9.2 Replacing the Motherboard (single node configuration)

D.1.10 Replacing the DVD Drive

D.1.10.1 Replacing the DVD Drive (cluster configuration)

D.1.10.2 Replacing the DVD Drive (single node configuration)

D.1.11 Replacing the CPU

D.1.11.1 Replacing the CPU (cluster configuration)

D.1.11.2 Replacing the CPU (single node configuration)

Copyright © 2011, 2014, Hitachi, Ltd.

D.1.12 Replacing the HDD Backplane Board
D.1.12.1 Replacing the HDD Backplane Board (cluster configuration)
D.1.12.2 Replacing the HDD Backplane Board (single node configuration)
D.1.13 Replacing the Front Panel Board
D.1.13.1 Replacing the Front Panel Board (cluster configuration)
D.1.13.2 Replacing the Front Panel Board (single node configuration)
D.1.14 Replacing the PS Backboard
D.1.14.1 Replacing the PS Backboard (cluster configuration)
D.1.14.2 Replacing the PS Backboard (single node configuration)
D.1.15 Replacing the Lithium Battery
D.1.15.1 Replacing the Lithium Battery (cluster configuration)
D.1.15.2 Replacing the Lithium Battery (single node configuration)
D.1.16 Replacing the PCI Riser Board
D.1.16.1 Replacing the PCI Riser Board (cluster configuration)
D.1.16.2 Replacing the PCI Riser Board (single node configuration)
D.1.17 Replacing the CPU Heatsink
D.1.17.1 Replacing the CPU Heatsink (cluster configuration)
D.1.17.2 Replacing the CPU Heatsink (single node configuration)
D.1.18 Replacing the CPU Air Duct
D.1.18.1 Replacing the CPU Air Duct (cluster configuration)
D.1.18.2 Replacing the CPU Air Duct (single node configuration)
D.1.19 Replacing the Cable
D.1.19.1 Replacing the Cable (cluster configuration)
D.1.19.2 Replacing the Cable (single node configuration)
D.1.20 Replacing the BMC
D.1.21 Replacing the Management Port
D.1.22 Replacing the Internal RAID Battery
D.1.23 Replacing the USB Board
D.1.24 Replacing the SFP module

Copyright © 2011, 2014, Hitachi, Ltd.

D.1 Replacing the Components

Table D.1-1 shows the parts to be replaced and the status of the OS operation to the node in replacement. The parts name of the hardware vendor is also shown in the following table because it must see "Hitachi Advanced Server 8000/RS220xK Maintenance Manual" depends on the parts to be replaced.

Table 1-1 Parts to be Replaced and the Status of the OS Operation to the Node in Replacement (1/3)

No.	Component	Hitachi Advanced Server 8000/RS220xK Maintenance Manual component name	Node configuration	Node OS operation status		Parts replacement	Approximate work time
				On (*2)	Off (*3)		
1	Power Supply unit	Power Supply	Cluster configuration	Y (*1)	Y	'D.1.1.1 Replacing the Power Supply Unit/ AC Cable (cluster configuration)'	30 minutes
			Single node configuration		Y	'D.1.1.2 Replacing the Power Supply Unit/ AC Cable (single node configuration)'	
2	Fan unit	System FAN	Cluster configuration	N	Y	'D.1.2.1 Replacing the Fan Unit (cluster configuration)'	30 minutes
			Single node configuration			'D.1.2.2 Replacing the Fan Unit (single node configuration)'	
3	Internal hard disk drive	HDD	Cluster configuration	Y (*1)	Y	'D.1.3.1 Replacing the Internal Hard Disk Drive (cluster configuration)'	90 minutes
			Single node configuration	Y (*4)		'D.1.3.2 Replacing the Internal Hard Disk Drive (single node configuration)'	
4	RAID Controller	6G SAS RAID card	Cluster configuration	N	Y	'D.1.4.1 Replacing the RAID Controller (cluster configuration)'	30 minutes
			Single node configuration			'D.1.4.2 Replacing the RAID Controller (single node configuration)'	
5	Memory	Memory Board	Cluster configuration	N	Y	'D.1.5.1 Replacing the Memory (cluster configuration)'	30 minutes
			Single node configuration			'D.1.5.2 Replacing the Memory (single node configuration)'	
6	Fibre Channel Card	PCI Cards	Cluster configuration	N	Y	'D.1.6.1 Replacing the Fibre Channel Card (cluster configuration)'	60 minutes
			Single node configuration			'D.1.6.2 Replacing the Fibre Channel Card (single node configuration)'	
7	GbE-4Port Card	PCI Cards	Cluster configuration	N	Y	'D.1.7.1 Replacing the GbE-4Port Card (cluster configuration)'	30 minutes
			Single node configuration			'D.1.7.2 Replacing the GbE-4Port Card (single node configuration)'	
8	GbE-2Port Card	PCI Cards	Cluster configuration	N	Y	'D.1.8.1 Replacing the GbE-2Port Card (cluster configuration)'	30 minutes
			Single node configuration			'D.1.8.2 Replacing the GbE-2Port Card (single node configuration)'	

*1: Replacement while the power is on is possible only in case of failure in one node. (Replacement must be performed while the power is off in case of failure in both nodes.)
*2: The node is in operation.
*3: The failover is being performed for the other node, and the user service continues.
*4: In the case of one failed HDD, it can be replaced while the power is turned on (in the case of two failed HDDs, they need to be replaced while the power is turned off. However, in the case of RAID6, even if the two HDDs failed, they can be replaced while the power is turned on).

Copyright © 2012, 2016, Hitachi, Ltd.

Table 1-1 Parts to be Replaced and the Status of the OS Operation to the Node in Replacement (2/3)

No.	Component	Hitachi Advanced Server 8000/RS220xK Maintenance Manual component name	Node configuration	Node OS operation status		Parts replacement	Approximate work time
				On (*2)	Off (*3)		
9	Motherboard	Mother Board	Cluster configuration	N	Y	'D.1.9.1 Replacing the Motherboard (cluster configuration)'	50 minutes
			Single node configuration			'D.1.9.2 Replacing the Motherboard (single node configuration)'	
10	DVD Drive	DVD-ROM Drive SFF SATA	Cluster configuration	N	Y	'D.1.10.1 Replacing the DVD Drive (cluster configuration)'	30 minutes
			Single node configuration			'D.1.10.2 Replacing the DVD Drive (single node configuration)'	
11	CPU	CPU	Cluster configuration	N	Y	'D.1.11.1 Replacing the CPU (cluster configuration)'	30 minutes
			Single node configuration			'D.1.11.2 Replacing the CPU (single node configuration)'	
12	HDD Backplane board	HDD Backplane	Cluster configuration	N	Y	'D.1.12.1 Replacing the HDD Backplane board (cluster configuration)'	60 minutes
			Single node configuration			'D.1.12.2 Replacing the HDD Backplane board (single node configuration)'	

*1: Replacement while the power is on is possible only in case of failure in one node. (Replacement must be performed while the power is off in case of failure in both nodes.)
*2: The node is in operation.
*3: The failover is being performed for the other node, and the user service continues.

Copyright © 2012, 2016, Hitachi, Ltd.

Table 1-1 Parts to be Replaced and the Status of the OS Operation to the Node in Replacement (3/3)

No.	Component	Hitachi Advanced Server 8000/RS220xK Maintenance Manual component name	Node configuration	Node OS operation status		Parts replacement	Approximate work time
				On *2	Off *3		
13	Front Panel Board	Front Panel Board	Cluster configuration	N	Y	'D.1.13.1 Replacing the Front Panel Board (cluster configuration)'	30 minutes
			Single node configuration			'D.1.13.2 Replacing the Front Panel Board (single node configuration)'	
14	PS Backboard	PS Backboard	Cluster configuration	N	Y	'D.1.14.1 Replacing the PS Backboard (cluster configuration)'	60 minutes
			Single node configuration			'D.1.14.2 Replacing the PS Backboard (single node configuration)'	
15	Lithium Battery	Lithium Battery	Cluster configuration	N	Y	'D.1.15.1 Replacing the Lithium Battery (cluster configuration)'	30 minutes
			Single node configuration			'D.1.15.2 Replacing the Lithium Battery (single node configuration)'	
16	PCI Riser Board	PCI Riser Boards	Cluster configuration	N	Y	'D.1.16.1 Replacing the PCI Riser Board (cluster configuration)'	30 minutes
			Single node configuration			'D.1.16.2 Replacing the PCI Riser Board (single node configuration)'	
17	CPU Heatsink	CPU Heatsink	Cluster configuration	N	Y	'D.1.17.1 Replacing the CPU Heatsink (cluster configuration)'	30 minutes
			Single node configuration			'D.1.17.2 Replacing the CPU Heatsink (single node configuration)'	
18	CPU Air Duct	CPU Air Duct	Cluster configuration	N	Y	'D.1.18.1 Replacing the CPU Air Duct (cluster configuration)'	30 minutes
			Single node configuration			'D.1.18.2 Replacing the CPU Air Duct (single node configuration)'	
19	Cable	One of the followings : •3.5" SAS Cable •SM BUS Cable •Front Panel Cable •DVD SATA Cable •3.5" FAN Cable Set •Front USB Cable •PS Backboard & Cable	Cluster configuration	N	Y	'D.1.19.1 Replacing the Cable (cluster configuration)'	30 minutes
			Single node configuration			'D.1.19.2 Replacing the Cable (single node configuration)'	
20	BMC	—	—	—	—	'D.1.20 Replacing the BMC'	—
21	Management Port	—	—	—	—	'D.1.21 Replacing the Management Port'	—
22	Internal RAID Battery	Battery Backup Unit	Single node configuration	N	Y	'D.1.22 Replacing the Internal RAID Battery'	30 minutes
23	USB board	—	—	—	—	'D.1.23 Replacing the USB Board'	—
24	SFP module	—	—	—	—	'D.1.24 Replacing the SFP module'	—

*1: Replacement while the power is on is possible only in case of failure in one node. (Replacement must be performed while the power is off in case of failure in both nodes.)
*2: The node is in operation.
*3: The failover is being performed for the other node, and the user service continues.

Copyright © 2012, 2016, Hitachi, Ltd.

D.1.1 Replacing the Power Supply Unit/ AC Cable

For the cluster configuration, refer to D.1.1.1 Replacing the Power Supply Unit/ AC Cable (cluster configuration). For the single node configuration, refer to ‘D.1.1.2 Replacing the Power Supply Unit/ AC Cable (single node configuration)’.

D.1.1.1 Replacing the Power Supply Unit/ AC Cable (cluster configuration)

Select either method:

Table D.1.1.1-1 Replacing a power supply unit

Method	Node status at replacement	Replacement procedure
1	The node is running.	(1) Replacement procedure while the node is in operation
2	The node is turned off.	(2) Replacement procedure while the node is turned off

Copyright © 2012, 2013, Hitachi, Ltd.

(1) Replacement procedure while the node is in operation

NOTE: When replacing AC cable, read the word of Power supply unit as AC cable.

(a) Refer to “Hitachi Advanced Server 8000/RS220xK Maintenance Manual” and replace the power supply unit.

NOTE: Precautions before the parts replacement

- When replacing power supply unit, replace it with the instruction described in “Hitachi Advanced Server 8000/RS220xK Maintenance Manual”.
- Simple log acquisition instructed in “Hitachi Advanced Server 8000/RS220xK Maintenance Manual” is unnecessary.

(b) After replacing the power supply unit, connect the power supply cable to check if the power source lamp is on in green. For the power supply lamp confirmation of the power supply unit, refer to “Hitachi Advanced Server 8000/RS220xK Maintenance Manual”.

(c) After the OS is started on the node, check the following:
Check the hardware status. Check whether “ok” is displayed for both 0 and 1 of “Power Supply Information” on the screen.
(For details about how to check the hardware status, refer to ‘B.3.1 Displaying the Hardware Status (hwstatus)’.)

Copyright © 2012, 2013, Hitachi, Ltd.

(2) Replacement procedure while the node is turned off

NOTE: When replacing AC cable, read the word of power supply unit as AC cable.

(a) Stop the OS on the target node.
For details about how to stop the OS on a node, refer to "Maintenance Tool '2.28 Terminating the OS of This Side Node (nasshutdown)' (MNTT 02-1740)".

(b) Refer to "Hitachi Advanced Server 8000/RS220xK Maintenance Manual" and replace the power supply unit.

NOTE: Precautions before the parts replacement
- When replacing power supply unit, replace it with the instruction described in "Hitachi Advanced Server 8000/RS220xK Maintenance Manual", and confirm the operation after the replacement by using HATP (a program that executes operation confirmation and executes determination when a failure occurs on HA8000 series).
- Depend on the result of HATP, other possible suspect parts might be replaced. In this case, return to 'C.2.2.1 Failure determination procedure at the cluster configuration' and determine the subject parts.

(c) When the replacement of the power supply unit is done by removing all the cables, reconnect the cables to the location as it were, and check that the power supply lamp of the power supply unit is blinking in green light. For the power supply lamp of the power supply unit, refer to "Hitachi Advanced Server 8000/RS220xK Maintenance Manual".

NOTE: When there has been an instruction to let the heartbeat cable and maintenance port cable removed during operation before executing the replacement procedure, do not connect heartbeat cable and the maintenance port cable and just connect the other cables.

(d) Turn on the Power lamp switch, and check that the power supply lamp is turned on in green light. In the case of the light color is other than green, take measures in accordance with the description in "Hitachi Advanced Server 8000/RS220xK Maintenance Manual", and then check the power supply lamp again. This procedure is unnecessary when the node is started by connecting cables at (f).

(e) Confirm that the OS startup of the node is complete.
Refer to "Set Up '1.3 Startup Confirmation of the OS by using KVM' (SETUP 01-0010)" and confirm that the login prompt window is displayed.
If the login prompt window is not displayed and a boot failure window is displayed, the OS startup was not successful because another failure occurred. Refer to 'C.2.4 Diagnosis for OS Boot Failure' and execute the solution to the failure. After the failure is solved, proceed to the step (f).
If the login prompt window is displayed, proceed to the step (f).

(f) Confirm the node status on the other side.
To check, execute the peerstatus command on the other (normal) node and check whether the status is [BOOT COMPLETE]. For details about how to check node status, refer to "Maintenance Tool '2.36 Displaying the Status of Other Side Node (peerstatus)' (MNTT 02-2130)".

NOTE: Wait approximately 10 minutes until the OS is completely started.

Copyright © 2012, 2013, Hitachi, Ltd.

(g) Check the hardware status.
Check the hardware status. Check whether “ok” is displayed for both 0 and 1 of “Power Supply Information” on the screen.
For details about how to check the hardware status, refer to ‘B.3.1 Displaying the Hardware Status (hwstatus)’.

(h) Return to the step (f) of “Replacement ‘1.1.1 Replacing the Power Supply Unit/ AC Cable (2) Replacement procedure while the node is turned off’ (REP 01-0040)”, and execute the rest of the procedures.

Copyright © 2011, 2013, Hitachi, Ltd.

D.1.1.2 Replacing the Power Supply Unit/ AC Cable (single node configuration)

Select either method:

Table D.1.1.2-1 Replacing a power supply unit

Method	Node status at replacement	Replacement procedure
1	The node is running.	(1) Replacement procedure while the node is in operation
2	The node is turned off.	(2) Replacement procedure while the node is turned off

Copyright © 2012, 2013, Hitachi, Ltd.

(1) Replacement procedure while the node is in operation

NOTE: When replacing AC cable, read the word of Power supply unit as AC cable.

(a) Refer to “Hitachi Advanced Server 8000/RS220xK Maintenance Manual” and replace the power supply unit.

NOTE: Precautions before the parts replacement

- When replacing power supply unit, replace it with the instruction described in “Hitachi Advanced Server 8000/RS220xK Maintenance Manual”.
- Simple log acquisition instructed in Hitachi Advanced Server 8000/RS220xK Maintenance Manual” is unnecessary.

(b) After replacing the power supply unit, connect the power supply cable to check if the power source lamp is on in green. For the power supply lamp confirmation of the power supply unit, refer to “Hitachi Advanced Server 8000/RS220xK Maintenance Manual”.

(c) After the OS is started on the node, check the following:
Check the hardware status. Check whether “ok” is displayed for both 0 and 1 of “Power Supply Information” on the screen.
(For details about how to check the hardware status, refer to ‘B.3.1 Displaying the Hardware Status (hwstatus)’.)

Copyright © 2012, 2013, Hitachi, Ltd.

(2) Replacement procedure while the node is turned off

(a) Stop the OS on the target node. Before stopping the OS of the node, ask the system administrator if the service can be stopped or not. After that confirmation, execute the operation.
For details about how to stop the OS on a node, refer to "Maintenance Tool '2.28 Terminating the OS of This Side Node (nasshutdown)' (MNTT 02-1740)".

(b) Refer to "Hitachi Advanced Server 8000/RS220xK Maintenance Manual" and replace the power supply unit.

NOTE: Precautions before the parts replacement

- When replacing power supply unit, replace it with the instruction described in "Hitachi Advanced Server 8000/RS220xK Maintenance Manual", and confirm the operation after the replacement by using HATP (a program that executes operation confirmation and executes determination when a failure occurs on HA8000 series).
- Depend on the result of HATP, other possible suspect parts might be replaced. In this case, return to 'C.2.2.2 Failure determination procedure at the single node configuration' and determine the subject parts.

(c) When the replacement of the power supply unit is done by removing all the cables, reconnect the cables to the location as it were, and check that the power supply lamp of the power supply unit turns on in green light. For the power supply lamp of the power supply unit, refer to "Hitachi Advanced Server 8000/RS220xK Maintenance Manual".

(d) Turn on the Power lamp switch, and check that the power supply lamp is turned on in green light. In the case of the light color is other than green, take measures in accordance with the description in "Hitachi Advanced Server 8000/RS220xK Maintenance Manual", and then check the power supply lamp again. This procedure is unnecessary when the node is started by connecting cables at (f).

(e) Confirm that the OS startup of the node is complete.
Refer to "Set Up '1.3 Startup Confirmation of the OS by using KVM' (SETUP 01-0010)" and confirm that the login prompt window is displayed.
If the login prompt window is not displayed and a boot failure window is displayed, the OS startup was not successful because another failure occurred. Refer to 'C.2.4 Diagnosis for OS Boot Failure' and execute the solution to the failure. After the failure is solved, proceed to the step (f).
If the login prompt window is displayed, proceed to the step (f).

NOTE: Wait approximately 10 minutes until the OS is completely started.

Copyright © 2012, 2013, Hitachi, Ltd.

(f) Check if the resource group is running normally.
Execute rgstatus command to confirm whether the resource group is running normally.
For the method for confirmation, refer to "Maintenance Tool '2.63 Resource group Status Display (rgstatus)' (MNTT 02-3380)".

(g) Check the hardware status.
Check the hardware status. Check whether "ok" is displayed for both 0 and 1 of "Power Supply Information" on the screen.
For details about how to check the hardware status, refer to 'B.3.1 Displaying the Hardware Status (hwstatus)'.

(h) Return to the step (d) of "Replacement '1.1.2 Replacing the Power Supply Unit/ AC cable (single node configuration) (2) Replacement procedure while the node is turned off' (REP 01-0060)" and execute the rest of the procedures.

Copyright © 2011, 2013, Hitachi, Ltd.

D.1.2 Replacing the Fan Unit

For the cluster configuration, refer to D.1.2.1 Replacing the Fan Unit (cluster configuration).
For the single node configuration, refer to 'D.1.2.2 Replacing the Fan Unit (single node configuration)'.

D.1.2.1 Replacing the Fan Unit (cluster configuration)

(1) Stop the OS on the target node.
For details about how to stop the OS on a node, refer to "Maintenance Tool '2.28 Terminating the OS of This Side Node (nasshutdown)' (MNTT 02-1740)".

(2) Refer to "Hitachi Advanced Server 8000/RS220xK Maintenance Manual" and replace the fan unit.

NOTE: Precautions before the parts replacement
- When replacing fan unit, replace it with the instruction described in "Hitachi Advanced Server 8000/RS220xK Maintenance Manual" and confirm the operation after the replacement by using HATP (a program that executes operation confirmation and executes determination when a failure occurs on HA8000 series).
- Depend on the result of HATP, the other possible suspect parts might be replaced. In this case, return to 'C.2.2.1 Failure determination procedure at the cluster configuration' and determine the subject parts.

(3) After replacing the fan unit, reconnect the cables where they were if they are all removed at the replacing operation, and press the power button on the node.

NOTE: When there has been an instruction to let the heartbeat cable and maintenance port cable removed during operation before executing the replacement procedure, do not connect heartbeat cable and the maintenance port cable and just connect the other cables.

(4) Confirm that the OS startup of the node is complete.
Refer to "Set Up '1.3 Startup Confirmation of the OS by using KVM' (SETUP 01-0010)" and confirm that the login prompt window is displayed.
If the login prompt window is not displayed and a boot failure window is displayed, the OS startup was not successful because another failure occurred. Refer to 'C.2.4 Diagnosis for OS Boot Failure' and execute the solution to the failure. After the failure is solved, proceed to the step (5). If the login prompt window is displayed, proceed to step (5).

(5) Confirm the node status on the other side.
To check, execute the peerstatus command on the other (normal) node and check whether the status is [BOOT COMPLETE].
For details about how to check node status, refer to "Maintenance Tool '2.36 Displaying the Status of Other Side Node (peerstatus)' (MNTT 02-2130)".

NOTE: Wait approximately 10 minutes until the OS is completely started.

(6) After the OS is started on the node, check the following item.
Check the hardware status. Check whether "ok" is displayed for all items of "FAN Information" on the screen. For details about how to check the hardware status, refer to 'B.3.1 Displaying the Hardware Status (hwstatus)'.

(7) Return to the step (e) of "Replacement '1.2.1 Parts replacement only when the node is turned off (cluster configuration)' (REP 01-0070)" and execute the rest of the procedures.

Copyright © 2012, 2013, Hitachi, Ltd.

D.1.2.2 Replacing the Fan Unit (single node configuration)

(1) Stop the OS on the target node.
Before stopping the OS of the node, ask the system administrator if the service can be stopped or not. After that confirmation, execute the operation.
For details about how to stop the OS on a node, refer to "Maintenance Tool '2.28 Terminating the OS of This Side Node (nasshutdown)' (MNTT 02-1740)".

(2) Refer to "Hitachi Advanced Server 8000/RS220xK Maintenance Manual" and execute fan unit replacement.

NOTE: Precautions before the parts replacement

- When replacing fan unit, replace it with the instruction described in "Hitachi Advanced Server 8000/RS220xK Maintenance Manual" and confirm the operation after the replacement by using HATP (a program that executes operation confirmation and executes determination when a failure occurs on HA8000 series).
- Depend on the result of HATP, the other possible suspect parts might be replaced. In this case, return to 'C.2.2.2 Failure determination procedure at the single node configuration' and determine the subject parts.

(3) After the fan unit replacement is complete, in case the replacement operation was performed by removing all the cables, reconnect the cables where they were, and then turn on the power supply button.

(4) Confirm that the OS startup of the node is complete.
Refer to "Set Up '1.3 Startup Confirmation of the OS by using KVM' (SETUP 01-0010)" and confirm that the login prompt window is displayed.
If the login prompt window is not displayed and a boot failure window is displayed, the OS startup was not successful because another failure occurred. Refer to 'C.2.4 Diagnosis for OS Boot Failure' and execute the solution to the failure. After the failure is solved, proceed to the step (5).
If the login prompt window is displayed, proceed to the step (5).

NOTE: Wait approximately 10 minutes until the OS is completely started.

(5) Check if the resource group is running normally.
Execute the rgstatus command to confirm whether the resource group is running normally. For the method for confirmation, refer to "Maintenance Tool '2.63 Resource group Status Display (rgstatus)' (MNTT 02-3380)".

(6) After the OS is started on the node, check the following.
Check the hardware status. Check whether "ok" is displayed for all items of "FAN Information" on the screen. (For checking the hardware status, refer to 'B.3.1 Displaying the Hardware Status (hwstatus)'.

(7) Return to the step (c) of "Replacement '1.2.2 Parts replacement only when the node is turned off (single node configuration)' (REP 01-0090)" and execute the rest of the procedures.

Copyright © 2012, 2013, Hitachi, Ltd.

D.1.3 Replacing the Internal Hard Disk Drive

For the cluster configuration, refer to D.1.3.1 Replacing the Internal Hard Disk Drive (cluster configuration).
For the single node configuration, refer to ‘D.1.3.2 Replacing the Internal Hard Disk Drive (single node configuration)’.

D.1.3.1 Replacing the Internal Hard Disk Drive (cluster configuration)

(1) Replacement procedure while the node is in operation (replacement of one internal HDD)

NOTE: You can confirm the logs/status in the replacement while the node is in operation in the following procedures by executing the command of MegaRAID Storage Manager (CLI version.) Therefore, you do not need to install MegaRAID Storage Manager (GUI version) or perform the operations in MegaRAID Storage Manager (GUI version), as described in the manual Maintenance Manual Hitachi Advanced Server 8000/RS220xK.
Remove the internal HDD to be replaced, and replace it with its maintenance part HDD.

(a) Check whether one of following SIM message is displayed. (Refer to “Maintenance Tool ‘2.6 Displaying SIMs on This Side (syseventlist)’ (MNTT 02-0360)”.)

- In the case of internal HDD failure, “KAQK30801-E MIACAT detected a failure (MAR=(MAR) RC=(RC))” is displayed. Therefore, confirm that if the RC is a failure code of the internal HDD with reference to “Hitachi Advanced Server 8000/RS220xK Maintenance Manual”.

- In the case of internal HDD failure, check the status of the hardware, and confirm the “InternalHDD Information” on the window shows “failed” in either of 0 and 1. (for the confirmation of the hardware, refer to ‘B.3.1 Displaying the Hardware Status (hwstatus)’.

- In the case of internal HDD preventing replacement, check if “KAQK37512-E The number of internal RAID device media errors has exceeded the threshold.(internal_disk_number)” or “KAQK37514-E The number of internal RAID device S.M.A.R.T. warnings has exceeded the threshold (internal_disk_number)” is displayed on the window.
  The extension storage bay number for the HDD of the subject to be replaced becomes the value of internal_disk_number as shown in the above message +1.
  For the location of installing the extension storage bay, refer to ‘A.2.1 Front side’.

Copyright © 2011, 2018, Hitachi, Ltd.

(b) Refer to "Maintenance Tool '2.56 Status Information Acquisition of the Virtual Disk and the Physical Disk (state.sh)' (MNTT 02-3110)," and collect the status information of the current internal HDD.

(c) Refer to "Maintenance Tool '2.55 Embedded RAID Controller Internal Log Acquisition (log.sh)' (MNTT 02-3080)", and confirm the obtained log.

(d) Refer to "Hitachi Advanced Server 8000/RS220xK Maintenance Manual" and execute internal hard disk drive replacement.

NOTE: Precautions before the parts replacement
When replacing internal HDD, replace it with the instruction described in "Hitachi Advanced Server 8000/RS220xK Maintenance Manual".

(e) Refer to "Maintenance Tool '2.58 Confirmation of Rebuilding Progress of Physical Disk (rbldchk.sh)' (MNTT 02-3170)", and confirm the rebuilding progress.

(f) After replacing the internal HDD, confirm the following items.

- Confirm that the LED of internal HDD turns on in green light. For the confirmation of the LED of internal HDD, refer to "Hitachi Advanced Server 8000/RS220xK Maintenance Manual".

- In the case of internal HDD preventing replacement, check if "KAQK37513-I The number of internal RAID device media errors has been cleared. (internal_disk_number) " or "KAQK37515-I The number of internal RAID device S.M.A.R.T. warnings has been cleared (internal_disk_number) " is displayed on the window. (for the confirmation of the message, refer to "Maintenance Tool '2.6 Displaying SIMs on This Side (syseventlist)' (MNTT 02-0360)".

- Check the hardware status. Check whether "ok" is displayed for both 0 and 1 of "InternalHDD Information" on the screen.
  For details about how to check the hardware status, refer to 'B.3.1 Displaying the Hardware Status (hwstatus)'.

The confirmation of the above items are all OK, the replacement procedure is complete.

Copyright © 2011, 2016, Hitachi, Ltd.

(2) Replacement procedure while the node is turned off (replacement of two internal HDDs)

(a) Stop the OS on the target node.
For details about how to stop the OS on a node, refer to "Maintenance Tool '2.28 Terminating the OS of This Side Node (nasshutdown)' (MNTT 02-1740)".

(b) Refer to "Hitachi Advanced Server 8000/RS220xK Maintenance Manual", and replace the internal HDD.
The power source must be stopped because the new installation is done after the replacement.

NOTE: Precautions before the parts replacement

- When replacing internal HDD, replace it with the instruction described in "Hitachi Advanced Server 8000/RS220xK Maintenance Manual" and confirm the operation after the replacement by using HATP (a program that executes operation confirmation and executes determination when a failure occurs on HA8000 series).
- Depend on the result of HATP, the other possible suspect parts might be replaced. In this case, return to 'C.2.2.1 Failure determination procedure at the cluster configuration' and determine the subject parts.
- Make sure to collect Simple log by using HATP before the replacement. For the details, refer to "Hitachi Advanced Server 8000/RS220xK Maintenance Manual."

(c) Execute newly installing the OS.
For the procedures, refer to "Set Up 'Chapter 3 New Installation' (SETUP 03-0000)".

(d) Perform settings after the installation is complete.
For the setting procedures, refer to "Set Up '5.1 Setting/ Confirmation after New Installation' (SETUP 05-0000)".

(e) Restore the OS.
For the procedures, refer to "Maintenance Tool '2.8 Recovering the Disk/Cluster Management LU (syslurestore)' (MNTT 02-0460)".

(f) Confirm the node status on the other side.
To check, execute the peerstatus command on the other (normal) node and check whether the status is [BOOT COMPLETE].
For details about how to check node status, refer to "Maintenance Tool '2.36 Displaying the Status of Other Side Node (peerstatus)' (MNTT 02-2130)".

NOTE: Wait approximately 10 minutes until the OS is completely started.

Copyright © 2012, 2013, Hitachi, Ltd.

(g) After the OS is started on the node, check the following items.

- Check whether the LEDs on the internal hard disk drive light green.
  For details about the color of the LEDs, refer to "HA8000/RS220xK Maintenance Manual".

- Check the hardware status. Check whether "ok" is displayed for both 0 and 1 of "InternalHDD Information" on the screen.
  For details about how to check the hardware status, refer to 'B.3.1 Displaying the Hardware Status (hwstatus)'.

(h) Return to the step (f) of the "Replacement '1.3.1 Replacing the Internal Hard Disk Drive (2) Replacement procedure while the node is turned off (replacement of two internal HDDs)' (REP 01-0130)" and execute the rest of the procedures.

Copyright © 2012, 2013, Hitachi, Ltd.

D.1.3.2 Replacing the Internal Hard Disk Drive (single node configuration)

NOTE: If the RAID level check of the internal HDD has not been finished yet, check it in advance. In case the node is in operation, refer to Internal HDD Information in 'B.3.1 Displaying the Hardware Status (hwstatus)'. Also, in case of the dual HDDs configuration, the above stated RAID level check is not required as the RAID level is fixed with RAID1.

Execute the procedure by selecting one of the following methods:

Table D.1.3.2-1 Replacing a power supply unit

Method	Node status at replacement	Replacement procedure
1	The node is in operation. (Replace 1 internal HDD (In case of RAID6 configuration, replace 1 or 2 HDDs))	(1) Replacement procedure while the node is in operation
2	The node is turned off. (In other than RAID6 configurations, replace 2 internal HDDs)	(2) Replacement procedure while the node is turned off

(1) Replacement procedure while the node is in operation

NOTE: You can confirm the logs/status in the replacement while the node is in operation in the following procedures by executing the command of MegaRAID Storage Manager (CLI version.) Therefore, you do not need to install MegaRAID Storage Manager (GUI version) or perform the operations in MegaRAID Storage Manager (GUI version), as described in the manual Maintenance Manual Hitachi Advanced Server 8000/RS220xK.
Remove the internal HDD to be replaced, and replace it with its maintenance part HDD.

(a) Check whether one of following SIM message is displayed. (Refer to "Maintenance Tool '2.6 Displaying SIMs on This Side (syseventlist)' (MNTT 02-0360)".)

- In the case of internal HDD failure, "KAQK30801-E MIACAT detected a failure (MAR=(MAR) RC=(RC))" is displayed. Therefore, confirm that if the RC is a failure code of the internal HDD with reference to "Hitachi Advanced Server 8000/RS220xK Maintenance Manual".

- In the case of internal HDD failure, check the status of the hardware, and confirm the "InternalHDD Information" on the window shows "failed" in either of 0 to 5. (for the confirmation of the hardware, refer to 'B.3.1 Displaying the Hardware Status (hwstatus)'.

- In the case of internal HDD preventing replacement, check if "KAQK37512-E The number of internal RAID device media errors has exceeded the threshold. (internal_disk_number)" or "KAQK37514-E The number of internal RAID device S.M.A.R.T. warnings has exceeded the threshold. (internal_disk_number)" is displayed on the window.
  The extension storage bay number for the HDD of the subject to be replaced becomes the value of internal_disk_number as shown in the above message +1.
  For the location of installing the extension storage bay, refer to 'A.2.1 Front side'.

Copyright © 2011, 2018, Hitachi, Ltd.

(b) Refer to "Maintenance Tool '2.56 Status Information Acquisition of the Virtual Disk and the Physical Disk (state.sh)' (MNTT 02-3110)," and collect the status information of the current internal HDD.

(c) When executing the internal HDD failure replacement or the OS version is 4.0.0-XX or earlier, this procedure is unnecessary. Proceed to the step (d).

When executing the internal HDD preventing replacement, refer to "Maintenance Tool '2.93 Consistency Checking of the Data in the Virtual Disk (ccstart.sh)' (MNTT 02-4960)," and execute Consistency Check.

NOTE: For detail of the length of consistency check processing time, refer to the following 'Approximate Time Required for Consistency Check'. And perform consistency check after gaining processing time agreement with the customer.

"HitachiAdvancedServer8000/RS220xK [RAID]"
--'1.HA8000/RS220KK (LSI SAS2108 Model)'
(HA8000 Series Maintenance Manual for Disk Array)
--'Time Required for Each Procedure' ('TOP(LSI RAID[SAS])')
--'Approximate Time Required for Consistency Check'

Capacity and RAID level of the replacement HDD, refer to the 'B.3.1 Displaying the Hardware Status (hwstatus)'.

(d) Refer to "Maintenance Tool '2.55 Embedded RAID Controller Internal Log Acquisition (log.sh)' (MNTT 02-3080)", and confirm the obtained log.

(e) Refer to "Hitachi Advanced Server 8000/RS220xK Maintenance Manual" and execute internal hard disk drive replacement. If a failure occurs in 2 HDDs, replace 2 HDDs.

NOTE: Precautions before the parts replacement
When replacing internal HDD, replace it with the instruction described in "Hitachi Advanced Server 8000/RS220xK Maintenance Manual".

(f) Refer to "Maintenance Tool '2.58 Confirmation of Rebuilding Progress of Physical Disk (rbldchk.sh)' (MNTT 02-3170)", and confirm the rebuilding progress.

(g) After replacing the internal HDD, confirm the following items.

- Confirm that the LED of internal HDD turns on in green light. For the confirmation of the LED of internal HDD, refer to "Hitachi Advanced Server 8000/RS220xK Maintenance Manual".

- In the case of internal HDD preventing replacement, check if "KAQK37513-I The number of internal RAID device media errors has been cleared. (internal_disk_number) " or "KAQK37515-I The number of internal RAID device S.M.A.R.T. warnings has been cleared. (internal_disk_number) " is displayed on the window. (For the confirmation of the message, refer to "Maintenance Tool '2.6 Displaying SIMs on This Side (syseventlist)' (MNTT 02-0360)".

- Check the hardware status. Check whether "ok" is displayed for both 0 and 1 of "InternalHDD Information" on the screen.
  For details about how to check the hardware status, refer to 'B.3.1 Displaying the Hardware Status (hwstatus)'.

The confirmation of the above items are all OK, the replacement procedure is complete.

Copyright © 2011, 2016, Hitachi, Ltd.

(2) Replacement procedure while the node is turned off

(a) Stop the OS on the target node. Before stopping the OS of the node, ask the system administrator if the service can be stopped or not. After that confirmation, execute the operation.
For details about how to stop the OS on a node, refer to "Maintenance Tool '2.28 Terminating the OS of This Side Node (nasshutdown)' (MNTT 02-1740)".

(b) Refer to "Hitachi Advanced Server 8000/RS220xK Maintenance Manual" and replace the internal hard disk drive.
The power source must be stopped because the initial OS installation will be executed after the replacement.

NOTE: Precautions before the parts replacement
- Make sure to collect Simple log by using HATP before the replacement. For the details, refer to "Hitachi Advanced Server 8000/RS220xK Maintenance Manual."
- When replacing internal HDD, replace it with the instruction described in "Hitachi Advanced Server 8000/RS220xK Maintenance Manual", and confirm the operation after the replacement by using HATP (a program that executes operation confirmation and executes determination when a failure occurs on HA8000 series).
- Depend on the result of HATP, other possible suspect parts might be replaced. In this case, return to 'C.2.2.2 Failure determination procedure at the single node configuration' and determine the subject parts.

(c) The procedure differs depending on the configuration.
- In case of the configuration connects to the disk array subsystem
  In case of the configuration using management port, refer to the procedure in Table D.1.3.2-2.
  In case of the configuration using trunk 2 Data ports, ask the system administrator for the location of a free port of the IP-SW which the customer configures. Then, refer to the following tables depending on the case.
  - If IP-SW has a free port, refer to Table D.1.3.2-3.
  - If IP-SW does not have a free port, refer to Table D.1.3.2-4.

- In case of the configuration which does not connect to the disk array subsystem
  In case of the configuration using management port, refer to the procedure in Table D.1.3.2-5.
  In case of the configuration using trunk 2 Data ports, ask the system administrator for the location of a vacant port of the IP-SW which the customer configures. Then, refer to the following tables depending on the case.
  - If IP-SW has a free port, refer to Table D.1.3.2-6.
  - If IP-SW does not have a free port, refer to Table D.1.3.2-7.

After completing the all referenced recovery procedure, proceed to the procedure (d).

Table D.1.3.2-2 Failure recovery procedures in the configuration using management port as well as connecting to the disk array subsystem

#	Process	Performed by	Reference
1	Execute the initial OS installation (without RAID reconfiguration)	Maintenance personnel	"Set up 'Chapter 3 New Installation' (SETUP 03-0000)"
2	Set after completing the installation	Maintenance personnel	"Set up '5.1 Setting/Confirmation after New Installation' (SETUP 05-0000)"
3	Execute the restoration of the OS area (recovery of user data is not required)	System administrator	—
4	Request I/O confirmation for the system	system administrator	—

Copyright ©2012, 2013, Hitachi, Ltd.

Table D.1.3.2-3 Failure recovery procedures in the Configuration using trunk 2 Data ports as well as connecting to the disk array subsystem (Free Port is Available in IP-SW)

#	Process	Performed by	Reference
1	Connect the free port confirmed with the system administrator and the management port of the node by the LAN cable.	Maintenance personnel	—
2	Execute the initial OS installation (without RAID reconfiguration).	Maintenance personnel	"Set up 'Chapter 3 New Installation' (SETUP 03-0000)"
3	Set after completing the installation (Set the IP address and the Routing that are used at the front-end LAN for the management port IP address. The IP address and the Routing that are used at the front-end LAN should be confirmed with the system administrator.)	Maintenance personnel	"Set up '5.1 Setting/Confirmation after New Installation' (SETUP 05-0000)"
4	Execute the restoration of the OS area (recovery of user data is not required)	System administrator	—
5	After completing the recovery, remove the LAN cable connected to the management port.	Maintenance personnel	—
6	Request I/O confirmation for the system	System administrator	—

Table D.1.3.2-4 Failure recovery procedures in the Configuration using trunk 2 Data ports as well as connecting to the disk array subsystem (Free Port is Not Available in IP-SW)

#	Process	Performed by	Reference
1	Disable VLAN/Link aggregation settings of IP-SW port which connecting to a node (ask the system administrator to leave a note of the settings so that the settings can be restored.).	System administrator	—
2	Remove a LAN cable from a node data port which is connecting to the IP-SW port which disabled at the above step #1 and reconnect to the management port.	Maintenance personnel	—
3	Execute the initial OS installation (without RAID reconfiguration).	Maintenance personnel	"Set up 'Chapter 3 New Installation' (SETUP 03-0000)"
4	Set after completing the installation. (For the management port IP address, set the IP address and routing used for the link aggregation. Ask the system administrator to confirm the IP address and routing used for the link aggregation.)	Maintenance personnel	"Set up '5.1 Setting/Confirmation after New Installation' (SETUP 05-0000)"
5	Execute the restoration of the OS area (recovery of user data is not required)	System administrator	—
6	After the completion of failure recovery, put the LAN cable which was reconnected at the above step #2 back to the original data port.	Maintenance personnel	—
7	Restore the IP-SW settings (VLAN/Link aggregation) changed at the above step #1.	System administrator	—
8	Request I/O confirmation for the system	System administrator	—

*1: KAQG81003-W is output after rebooting at the time of the system LU recovery. However no particular action is required. Continue the recovery procedure.

Copyright © 2012, 2013, Hitachi, Ltd.

Table D.1.3.2-5 Failure recovery procedures in the Configuration using management port as well as not connecting to the disk array subsystem

#	Process	Performed by	Reference
1	Execute a new OS installation (with RAID reconfiguration) (*1)	Maintenance personnel	"Set up 'Chapter 3 New Installation' (SETUP 03-0000)"
2	Set after completing the installation	Maintenance personnel	"Set up '5.1 Setting/Confirmation after New Installation' (SETUP 05-0000)"
3	Execute the restoration of the OS area and the user data.	System administrator	—
4	Confirm that no error message related to the file system or the file sharing is output	System administrator	—
5	In the configuration of HDI for Cloud, confirm if the file configuration is consistent between the HDI and the HCP after performing the restoration by executing the CLI command open to the system administrator.	System administrator	—
6	Request I/O confirmation for the system	System administrator	—

*1: All data in a node will be initialized.

Table D.1.3.2-6 Failure recovery procedures in the Configuration using trunk 2 Data ports as well as not connecting to the disk array subsystem (Data recovery using management port)

#	Process	Performed by	Reference
1	Connect the free port confirmed with the system administrator and the management port of the node by the LAN cable.	Maintenance personnel	—
2	Execute a new OS installation (with RAID reconfiguration) (*1)	Maintenance personnel	"Set up 'Chapter 3 New Installation' (SETUP 03-0000)"
3	Set after completing the installation (In the configuration of HDI for Cloud, set the IP address and the Routing that are used at the front-end LAN for the management port IP address. The IP address and the Routing that are used at the front-end LAN should be confirmed with the system administrator.)	Maintenance personnel	"Set up '5.1 Setting/Confirmation after New Installation' (SETUP 05-0000)"
4	Execute the restoration of the OS area and the user data.	System administrator	—
5	After completing the recovery, remove the LAN cable connected to the management port	Maintenance personnel	—
6	Confirm that no error message related to the file system or the file sharing is output	System administrator	—
7	In the configuration of HDI for Cloud, confirm if the file configuration is consistent between the HDI and the HCP after performing the restoration by executing the CLI command open to the system administrator.	System administrator	—
8	Request I/O confirmation for the system	System administrator	—

*1: All data in a node will be initialized.

Copyright © 2013, Hitachi, Ltd.

Table D.1.3.2-7 Failure recovery procedures in the Configuration using trunk 2 Data ports as well as not connecting to the disk array subsystem (Data recovery using data port)

#	Process	Performed by	Reference
1	Disable VLAN/Link aggregation settings of IP-SW port which connecting to a node (ask the system administrator to leave a note of the settings so that the settings can be restored.).	System administrator	—
2	If the OS version is 4.0.1-XX or earlier, remove a LAN cable from a node data port which is connecting to the IP-SW port which disabled at the above step #1 and reconnect to the management port.	Maintenance personnel	—
3	Execute a new OS installation (with RAID reconfiguration) (*1)	Maintenance personnel	"Set up 'Chapter 3 New Installation' (SETUP 03-0000)"
4	Set after completing the installation.	Maintenance personnel	"Set up '5.1 Setting/Confirmation after New Installation' (SETUP 05-0000)"
5	Execute the restoration of the OS area and the user data.	System administrator	—
6	If a LAN cable was reconnected at the above step #2 after the failure recovery, put the LAN cable back to the original data port.	Maintenance personnel	—
7	Restore the IP-SW settings (VLAN/Link aggregation) changed at the above step #1.	System administrator	—
8	Confirm that no error message related to the file system or the file sharing is output	System administrator	—
9	In the configuration of HDI for Cloud, confirm if the file configuration is consistent between the HDI and the HCP after performing the restoration by using the CLI command open to the system administrator.	System administrator	—
10	Request I/O confirmation for the system	System administrator	—

*1: All data in a node will be initialized.

(d) Check if the resource group is running normally.
Execute the rgstatus command to confirm whether the resource group is running normally. For the method for confirmation, refer to "Maintenance Tool '2.63 Resource group Status Display (rgstatus)' (MNTT 02-3380)".

(e) After replacing the internal HDD, confirm the following items.

- Confirm that the LED of internal HDD turns on in green light. For the confirmation of the LED of internal HDD, refer to "Hitachi Advanced Server 8000/RS220xK Maintenance Manual".

- Check the hardware status. Check whether "ok" is displayed for "InternalHDD Information" on the screen.
  For details about how to check the hardware status, refer to 'B.3.1 Displaying the Hardware Status (hwstatus)'.

If the confirmation of the above items are all OK, the replacement procedure is complete.

Copyright © 2013, Hitachi, Ltd.

D.1.4 Replacing the RAID Controller

For the cluster configuration, refer to D.1.4.1 Replacing the RAID Controller (cluster configuration).
For the single node configuration, refer to 'D.1.4.2 Replacing the RAID Controller (single node configuration)'.

D.1.4.1 Replacing the RAID Controller (cluster configuration)

(1) Stop the OS on the target node.
For details about how to stop the OS on a node, refer to "Maintenance Tool '2.28 Terminating the OS of This Side Node (nasshutdown)' (MNTT 02-1740)".

(2) Refer to "Hitachi Advanced Server 8000/RS220xK Maintenance Manual" and replace the RAID controller.

NOTE: Precautions before the parts replacement

- When replacing RAID controller, replace it with the instruction described in "Hitachi Advanced Server 8000/RS220xK Maintenance Manual" and confirm the operation after the replacement by using HATP (a program that executes operation confirmation and executes determination when a failure occurs on HA8000 series).
- Depend on the result of HATP, the other possible suspect parts might be replaced. In this case, return to 'C.2.2.1 Failure determination procedure at the cluster configuration' and determine the subject parts.
- Make sure to collect Simple log by using HATP before the replacement. For the details, refer to "Hitachi Advanced Server 8000/RS220xK Maintenance Manual."
- Write mode before replacement is taken over to the write mode after replacement. Write through will be set in VD0 (OS LU).

(3) After replacing the RAID controller, reconnect the cables where they were if they are all removed at the replacing operation, and press the power button on the node.

NOTE: When there has been an instruction to let the heartbeat cable and maintenance port cable removed during operation before executing the replacement procedure, do not connect heartbeat cable and the maintenance port cable and just connect the other cables.

(4) Confirm that the OS startup of the node is complete.
Check whether the OS is completely started on the node. To check, execute the peerstatus command on the other (normal) node and check whether the status is [BOOT COMPLETE].
For details about how to check node status, refer to "Maintenance Tool '2.36 Displaying the Status of Other Side Node (peerstatus)' (MNTT 02-2130)".

NOTE: Wait approximately 10 minutes until the OS is completely started.

(5) Confirm the firmware version of the RAID controller.
Refer to "Maintenance Tool '2.46 Confirming the Built-in RAID Controller Firmware Version (internalraidfwget)' (MNTT 02-2610)," and check the firmware version of the RAID controller.
For the version confirmation, refer to Version Management Table (Web).
When the firmware version of the RAID controller is the version that is required to update, refer to "Maintenance Tool '2.47 Updating the Built-in RAID Controller Firmware (internalraidfwupdate)' (MNTT 02-2640)," and update the firmware.
When the firmware version of the RAID controller does not require updating, proceed to step (7).

(6) Return to the step (e) of "Replacement '1.2.1 Parts replacement only when the node is turned off (cluster configuration)' (REP 01-0070)" and execute the rest of the procedures.

Copyright © 2012, 2013, Hitachi, Ltd.

D.1.4.2 Replacing the RAID Controller (single node configuration)

(1) Stop the OS on the target node.
Before stopping the OS of the node, ask the system administrator if the service can be stopped or not. After that confirmation, execute the operation.
For details about how to stop the OS on a node, refer to "Maintenance Tool '2.28 Terminating the OS of This Side Node (nasshutdown)' (MNTT 02-1740)".

(2) Refer to "Hitachi Advanced Server 8000/RS220xK Maintenance Manual" and replace the RAID controller.

NOTE: Precautions before the parts replacement

- When replacing RAID controller, replace it with the instruction described in "Hitachi Advanced Server 8000/RS220xK Maintenance Manual" and confirm the operation after the replacement by using HATP (a program that executes operation confirmation and executes determination when a failure occurs on HA8000 series).
- Depend on the result of HATP, the other possible suspect parts might be replaced. In this case, return to 'C.2.2.2 Failure determination procedure at the single node configuration' and determine the subject parts.
- Make sure to collect Simple log by using HATP before the replacement. For the details, refer to "Hitachi Advanced Server 8000/RS220xK Maintenance Manual."
- Write mode before replacement is taken over to the write mode after replacement.
  In case that a node and UPS are connected and also connected to the disk array, write through will be set to all VDs.
  If node and UPS are not connected and not connected to the disk array either, write through will be set toVD0 (OS LU), and write back will be set to VD2 (User LU).
  In case the node and UPS are not connected, write through will be set to all VDs.

(3) After replacing the RAID controller, reconnect the cables where they were if they are all removed at the replacing operation, and press the power button on the node.

(4) Confirm that the OS startup of the node is complete.
Refer to "Set Up '1.3 Startup Confirmation of the OS by using KVM' (SETUP 01-0010)" and confirm that the login prompt window is displayed.

NOTE: Wait approximately 10 minutes until the OS is completely started.

(5) Check if the resource group is running normally.
Execute the rgstatus command to confirm whether the resource group is running normally. For the method for confirmation, refer to "Maintenance Tool '2.63 Resource group Status Display (rgstatus)' (MNTT 02-3380)".

(6) Confirm the firmware version of the RAID controller.
Refer to "Maintenance Tool '2.46 Confirming the Built-in RAID Controller Firmware Version (internalraidfwget)' (MNTT 02-2610)," and check the firmware version of the RAID controller.
For the version confirmation, refer to Version Management Table (Web).
When the firmware version of the RAID controller is the version that is required to update, refer to "Maintenance Tool '2.47 Updating the Built-in RAID Controller Firmware (internalraidfwupdate)' (MNTT 02-2640)," and update the firmware.
When the firmware version of the RAID controller does not require updating, proceed to the following step.
If the OS version is 3.0.0-XX or later, proceed to step (7).
If the OS version is 2.2.0-XX or earlier, proceed to step (9).

Copyright © 2012, 2013, Hitachi, Ltd.

(7) Check the set value for automatically relearn performing of the Internal RAID Battery.
If the OS version is 3.0.0-XX, execute bbuautolearnget command to confirm [Auto-Learn Mode] is [Enabled].
If the OS version is 3.0.1-XX or later, execute bburelearnget command to confirm “Status” is [Enable].
For the details about bbuautolearnget command, refer to “Maintenance Tool ‘2.68 Displaying the Set Value for Automatically Relearn Performing of the Internal RAID Battery (bbuautolearnget)’ (MNTT 02-3650)”.
For the details about bburelearnget command, refer to “Maintenance Tool ‘2.86 Displaying Relearn Schedule of Cache Backup Module and Setting Status (enabled/disabled) of Schedule Execution (bburelearnget)’ (MNTT 02-4500)”.

When [Auto-Learn Mode] is [Enabled] or “Status” is [Enable], proceed to step (9).
When [Auto-Learn Mode] is [Disabled] or “Status” is [Enable], proceed to step (8).

(8) Change the set value for automatically relearn performing of the Internal RAID Battery.
If the OS version is 3.0.0-XX, execute “bbuautolearnset --on” command and after that perform step (7) again.
If the OS version is 3.0.1-XX or later, execute “bburelearnset --enable” command and after that perform step (7) again.
For the details about bbuautolearnset command, refer to “Maintenance Tool ‘2.67 Setting for Automatically Relearn Performing of the Internal RAID Battery (bbuautolearnset)’ (MNTT 02-3620)”.
For the details about bburelearnset command, refer to “Maintenance Tool "2.87 Setting Relearn Schedule of Cache Backup Module and Enabling/disabling Schedule Execution (bburelearnset)" (MNTT 02-4530)”.

(9) Collect the OS log of the node.
For the details about OS collection, refer to “Maintenance Tool ‘2.19 Collecting Logs (oslogget)’ (MNTT 02-1300)”.
If the OS version is 3.0.0-XX or later, proceed to step(10).
If the OS version is 2.2.0-XX or earlier, the replacement is complete by this step.

(10) Request the system administrator to check the cache writing mode setting when the battery level of the embedded RAID battery is low.

Copyright © 2012, 2014, Hitachi, Ltd.

D.1.5 Replacing the Memory

For the cluster configuration, refer to D.1.5.1 Replacing the Memory (cluster configuration).
For the single node configuration, refer to 'D.1.5.2 Replacing the Memory (single node configuration)'.

D.1.5.1 Replacing the Memory (cluster configuration)

(1) Stop the OS on the target node.
For details about how to stop the OS on a node, refer to "Maintenance Tool '2.28 Terminating the OS of This Side Node (nasshutdown)' (MNTT 02-1740)".

(2) Refer to "Hitachi Advanced Server 8000/RS220xK Maintenance Manual" and replace the memory.

NOTE: Precautions before the parts replacement
- When replacing memory, replace it with the instruction described in "Hitachi Advanced Server 8000/RS220xK Maintenance Manual" and confirm the operation after the replacement by using HATP (a program that executes operation confirmation and executes determination when a failure occurs on HA8000 series).
- Depend on the result of HATP, the other possible suspect parts might be replaced. In this case, return to 'C.2.2.1 Failure determination procedure at the cluster configuration' and determine the subject parts.
- Make sure to collect Simple log by using HATP before the replacement. For the details, refer to "Hitachi Advanced Server 8000/RS220xK Maintenance Manual."

(3) After replacing the memory, reconnect the cables where they were if they are all removed at the replacing operation, and press the power button on the node.

NOTE: When there has been an instruction to let the heartbeat cable and maintenance port cable removed during operation before executing the replacement procedure, do not connect heartbeat cable and the maintenance port cable and just connect the other cables.

(4) Confirm that the OS startup of the node is complete.
Refer to "Set Up '1.3 Startup Confirmation of the OS by using KVM' (SETUP 01-0010)" and confirm that the login prompt window is displayed.
If the login prompt window is not displayed and a boot failure window is displayed, the OS startup was not successful because another failure occurred. Refer to 'C.2.4 Diagnosis for OS Boot Failure' and execute the solution to the failure. After the failure is solved, proceed to the step (5). If the login prompt window is displayed, proceed to step (5).

(5) Confirm the node status on the other side.
To check, execute the peerstatus command on the other side (normal) node and check whether the status is [BOOT COMPLETE].
For details about how to check node status, refer to "Maintenance Tool '2.36 Displaying the Status of Other Side Node (peerstatus)' (MNTT 02-2130)".

NOTE: Wait approximately 10 minutes until the OS is completely started.

(6) After the OS is started on the node, check the hardware status. Confirm whether "installed" is displayed for the status of where the memory replacement was executed in "Memory Information" on the screen. (For details about how to check the hardware status, refer to 'B.3.1 Displaying the Hardware Status (hwstatus)'.)

(7) Return to the step (e) of "Replacement '1.2.1 Parts replacement only when the node is turned off (cluster configuration)' (REP 01-0070)"and execute the rest of procedures.

Copyright © 2012, 2013, Hitachi, Ltd.

D.1.5.2 Replacing the Memory (single node configuration)

(1) Stop the OS on the target node.
Before stopping the OS of the node, ask the system administrator if the service can be stopped or not. After that confirmation, execute the operation.
For details about how to stop the OS on a node, refer to "Maintenance Tool '2.28 Terminating the OS of This Side Node (nasshutdown)' (MNTT 02-1740)".

(2) Refer to "Hitachi Advanced Server 8000/RS220xK Maintenance Manual" and replace the memory.

NOTE: Precautions before the parts replacement

- When replacing memory, replace it with the instruction described in "Hitachi Advanced Server 8000/RS220xK Maintenance Manual" and confirm the operation after the replacement by using HATP (a program that executes operation confirmation and executes determination when a failure occurs on HA8000 series).
- Depend on the result of HATP, the other possible suspect parts might be replaced. In this case, return to 'C.2.2.2 Failure determination procedure at the single node configuration' and determine the subject parts.
- Make sure to collect Simple log by using HATP before the replacement. For the details, refer to "Hitachi Advanced Server 8000/RS220xK Maintenance Manual."

(3) After replacing the memory, reconnect the cables where they were if they are all removed at the replacing operation, and press the power button on the node.

(4) Confirm that the OS startup of the node is complete.
Refer to "Set Up '1.3 Startup Confirmation of the OS by using KVM' (SETUP 01-0010)" and confirm that the login prompt window is displayed.
If the login prompt window is not displayed and a boot failure window is displayed, the OS startup was not successful because another failure occurred. Refer to 'C.2.4 Diagnosis for OS Boot Failure' and execute the solution to the failure. After the failure is solved, proceed to the step (5). If the login prompt window is displayed, proceed to step (5).

NOTE: Wait approximately 10 minutes until the OS is completely started.

(5) Check if the resource group is running normally.
Execute the rgstatus command to confirm whether the resource group is running normally. For the method for confirmation, refer to "Maintenance Tool '2.63 Resource group Status Display (rgstatus)' (MNTT 02-3380)".

(6) After the OS is started on the node, check the hardware status. Confirm whether "installed" is displayed for the status of where the memory replacement was executed in "Memory Information" on the screen. (For details about how to check the hardware status, refer to 'B.3.1 Displaying the Hardware Status (hwstatus)'.)

(7) Return to the step (c) of "Replacement '1.2.2 Parts replacement only when the node is turned off (single node configuration)' (REP 01-0090)" and execute the rest of procedures.

Copyright © 2012, 2013, Hitachi, Ltd.

D.1.6 Replacing the Fibre Channel Card

For the cluster configuration, refer to D.1.6.1 Replacing the Fibre Channel Card (cluster configuration).
For the single node configuration, refer to 'D.1.6.2 Replacing the Fibre Channel Card (single node configuration)'.

D.1.6.1 Replacing the Fibre Channel Card (cluster configuration)

(1) Stop the OS on the target node.
For details about how to stop the OS on a node, refer to "Maintenance Tool '2.28 Terminating the OS of This Side Node (nasshutdown)' (MNTT 02-1740)".
When replacing FC card due to occurrence of cluster management LU failure or the both paths failures of the target node, execute nasshutdown command with "—force" option attached.
When the setting of host group security mode is enabled, execute the operation from the step (2).
When the setting of host group security mode is disabled, execute the operation from the step (3).

(2) You need to change the WWNs after replacing the Fibre Channel card. Record the WWNs written on the new card.

NOTE:
- The Fibre Channel card has one WWN corresponding to the "PORT 0" and the other WWN corresponding to the "PORT 1", which are written after the "IEEE ADDRESS" in the back of the card. Make sure you clearly identify the WWN of each port.
- Each WWN written on the Fibre Channel card consists of 12 digits and the first four digits (1000) are omitted. Therefore, when you record a WWN, add 1000 at the beginning and make sure the WWN is 16 digits.

(3) Disconnect all the Fibre Channel cables from the Fibre Channel card.

(4) Refer to "Hitachi Advanced Server 8000/RS220xK Maintenance Manual" and replace the Fibre Channel card. After the replacement, the power source must be stopped because the connection of Fibre Channel cable and the setting of the host group security are required to be set.

NOTE: Precautions before the parts replacement
- When replacing the Fibre Channel card to be installed in the expansion slot 2, replace the standard bracket that attached to the maintenance part with the Low Profile bracket and screws that attached to the failure part.
- When replacing the Fibre Channel card, replace it with the instruction described in "Hitachi Advanced Server 8000/RS220xK Maintenance Manual" and confirm the operation after the replacement by using HATP (a program that executes operation confirmation and executes determination when a failure occurs on HA8000 series).
- Depend on the result of HATP, the other possible suspect parts might be replaced. In this case, return to 'C.2.2.1 Failure determination procedure at the cluster configuration' and determine the subject parts.
- Make sure to collect Simple log by using HATP before the replacement. For the details, refer to "Hitachi Advanced Server 8000/RS220xK Maintenance Manual."

(5) When the setting of host group security mode is enabled, write down the WWNs of the parts that are removed at the step (4).
When the setting of the host group security mode is disabled, execute the operation from the step (8).

NOTE: Each WWN written on the Fibre Channel card consists of 12 digits and the first four digits (1000) are omitted. Therefore, when you record a WWN, add 1000 at the beginning and make sure the WWN is 16 digits.

Copyright © 2012, 2013, Hitachi, Ltd.

(6) To change the WWNs registered to the connection ports on the disk array subsystem, refer to "LUN Manager User's Guide" for the AMS2000 series or HUS100 series, and if USP V, USP VM, VSP, VSP G1000, or HUS VM is connected, refer to "5.3.1.4. LUN Management" in the installation section of the maintenance manual of each system, and if VSP Gx00/VSP Fx00 is connected, refer to "System Administrator Guide" for VSP Gx00/VSP Fx00. To change the WWNs, delete the WWNs recorded in step (5) and then register the WWNs recorded in step (2).
Change the WWN registered for each connection destination port.

(7) After completion of step (6), if the FC-SW is not used, skip this step. If the FC-SW is used, request the system administrator to change the FC-SW WWN zoning by deleting the WWN that you took a note of in step (5) and registering the WWN that you took a note of in step (2).

(8) After replacing the Fibre Channel card and changing the WWNs, connect the Fibre Channel cables to the new Fibre Channel card and press the power button on the node. If the cables are all removed at the replacing operation, reconnect them where they were and press the power button on the node.

NOTE: When there has been an instruction to let the heartbeat cable and maintenance port cable removed during operation before executing the replacement procedure, do not connect heartbeat cable and the maintenance port cable and just connect the other cables.

(9) After the OS is started, log in the node from the maintenance PC. It normally takes approximately 10 minutes until the OS is completely started. For the login, refer to "Maintenance Tool '1.3.2 Logging in to a node for executing commands' (MNTT 01-0200)".

NOTE: You can log in the node from the maintenance PC even if communication with the array was not restored after the FC card replacement. However, in that case, do not execute the commands that affect cluster operation such as clstatus command, etc.

(10) Confirm that the port of Fibre Channel card linked up.
- Check the LED statuses on the new Fibre Channel card. Make sure at least one port is linked up.
  Refer to "Hitachi Advanced Server 8000/RS220xK [I/O Adapter]" for how to check the LED indication.

(11) Execute fpstatus command. If "Status" of both paths is "Error", do not execute the rest of the procedures, return to Troubleshooting where you were originally referring to and execute the rest of the procedures there. For the fpstatus command, refer to "Maintenance Tool '2.5 Displaying the FC Status (fpstatus)' (MNTT 02-0280)".

(12) Check the version of the firmware. For the version confirmation, refer to the version control table (Web). Depending on the version of the firmware, you may need to downgrade the firmware.
For details about how to check the version of firmware, refer to "Maintenance Tool '2.24 Checking the HBA Firmware Version (fchbafwlist)' (MNTT 02-1600)".

(13) When the version of the firmware is appropriate, go to step (15).
If the version of the firmware is inappropriate, downgrade the firmware. For details about how to downgrade firmware, refer to "Maintenance Tool '2.25 Updating the HBA Firmware (fchbafwupdate)' (MNTT 02-1630)".

(14) After you downgrade the firmware, check its version.

(15) Return to the step (e) of "Replacement '1.2.1 Parts replacement only when the node is turned off (cluster configuration)' (REP 01-0070)", and execute the rest of the procedures.

Copyright © 2012, 2016, Hitachi, Ltd.

D.1.6.2 Replacing the Fibre Channel Card (single node configuration)

(1) Stop the OS on the target node. Before stopping the OS of the node, ask the system administrator if the service can be stopped or not. After that confirmation, execute the operation.
For details about how to stop the OS on a node, refer to "Maintenance Tool '2.28 Terminating the OS of This Side Node (nasshutdown)' (MNTT 02-1740)".
When replacing FC card due to occurrence of the both paths failures of the target node, execute nasshutdown command with "—force" option attached.
When the setting of host group security mode is enabled, execute the operation from the step (2).
When the setting of host group security mode is disabled, execute the operation from the step (3).

(2) You need to change the WWNs after replacing the Fibre Channel card. Record the WWNs written on the new card.

NOTE:
- The Fibre Channel card has one WWN corresponding to the "PORT 0" and the other WWN corresponding to the "PORT 1", which are written after the "IEEE ADDRESS" in the back of the card. Make sure you clearly identify the WWN of each port.
- Each WWN written on the Fibre Channel card consists of 12 digits and the first four digits (1000) are omitted. Therefore, when you record a WWN, add 1000 at the beginning and make sure the WWN is 16 digits.

(3) Disconnect all the Fibre Channel cables from the Fibre Channel card.

(4) Refer to "Hitachi Advanced Server 8000/RS220xK Maintenance Manual" and replace the Fibre Channel card. After the replacement, the power source must be stopped because the connection of Fibre Channel cable and the setting of the host group security are required to be set.

NOTE: Precautions before the parts replacement
- When replacing the Fibre Channel card to be installed in the expansion slot 2, replace the standard bracket that attached to the maintenance part with the Low Profile bracket and screws that attached to the failure part.
- When replacing Fibre Channel card, replace it with the instruction described in "Hitachi Advanced Server 8000/RS220xK Maintenance Manual" and confirm the operation after the replacement by using HATP (a program that executes operation confirmation and executes determination when a failure occurs on HA8000 series).
- Depend on the result of HATP, the other possible suspect parts might be replaced. In this case, return to 'C.2.2.2 Failure determination procedure at the single node configuration' and determine the subject parts.
- Make sure to collect Simple log by using HATP before the replacement. For the details, refer to "Hitachi Advanced Server 8000/RS220xK Maintenance Manual."

(5) When the setting of host group security mode is enabled, write down the WWNs of the parts that are removed at the step (4).
When the setting of the host group security mode is disabled, execute the operation from the step (7).

NOTE: Each WWN written on the Fibre Channel card consists of 12 digits and the first four digits (1000) are omitted. Therefore, when you record a WWN, add 1000 at the beginning and make sure the WWN is 16 digits.

Copyright ©2012, 2013, Hitachi, Ltd.

(6) To change the WWNs registered to the connection ports on the disk array subsystem, refer to "LUN Manager User's Guide" for the AMS2000 series or HUS100 series, and if USP V, USP VM, VSP, VSP G1000, or HUS VM is connected, refer to "5.3.1.4. LUN Management" in the installation section of the maintenance manual of each system, and if VSP Gx00/VSP Fx00 is connected, refer to "System Administrator Guide" for VSP Gx00/VSP Fx00. To change the WWNs, delete the WWNs recorded in step (5) and then register the WWNs recorded in step (2).
Change the WWN registered for each connection destination port.

(7) After replacing the Fibre Channel card and changing the WWNs, connect the Fibre Channel cables to the new Fibre Channel card and press the power button on the node. If the cables are all removed at the replacing operation, reconnect them where they were and press the power button on the node.

(8) After the OS is started, log in the node from the maintenance PC. It normally takes approximately 10 minutes until the OS is completely started. For the login, refer to "Maintenance Tool '1.3.2 Logging in to a node for executing commands' (MNTT 01-0200)".

NOTE: You can log in the node from the maintenance PC even if communication with the array was not restored after the FC card replacement.

(9) After the OS is started, check the following.
- Check the LED statuses on the new Fibre Channel card. Make sure at least one port is linked up.
  Refer to "Hitachi Advanced Server 8000/RS220xK [I/O Adapter]" for how to check the LED indication.

(10) Execute fpstatus command. If "Status" of both paths is "Error", do not execute the rest of the procedures, return to Troubleshooting where you were originally referring to and execute the rest of the procedures there. For the fpstatus command, refer to "Maintenance Tool '2.5 Displaying the FC Status (fpstatus)' (MNTT 02-0280)".

(11) Check the version of the firmware. For the version confirmation, refer to the version control table (Web). Depending on the version of the firmware, you may need to downgrade the firmware.
For details about how to check the version of firmware, refer to "Maintenance Tool '2.24 Checking the HBA Firmware Version (fchbafwlist)' (MNTT 02-1600)".

(12) When the version of the firmware is appropriate, go to step (14).
If the version of the firmware is inappropriate, downgrade the firmware. For details about how to downgrade firmware, refer to "Maintenance Tool '2.25 Updating the HBA Firmware (fchbafwupdate)' (MNTT 02-1630)".

(13) After you downgrade the firmware, check its version.

(14) Return to the step (c) of "Replacement '1.2.2 Parts replacement only when the node is turned off (single node configuration)' (REP 01-0090)", and execute the rest of the procedures.

Copyright © 2012, 2016, Hitachi, Ltd.

D.1.7 Replacing the GbE-4Port Card

For the cluster configuration, refer to D.1.7.1 Replacing the GbE-4Port Card (cluster configuration).
For the single node configuration, refer to 'D.1.7.2 Replacing the GbE-4Port Card (single node configuration)'.

D.1.7.1 Replacing the GbE-4Port Card (cluster configuration)

(1) Stop the OS on the target node.
For details about how to stop the OS on a node, refer to "Maintenance Tool '2.28 Terminating the OS of This Side Node (nasshutdown)' (MNTT 02-1740)".

(2) Disconnect all the LAN cables from the GbE-4Port card.

(3) Refer to "Hitachi Advanced Server 8000/RS220xK Maintenance Manual" and replace the GbE-4Port card.
After the replacement, the power source must be stopped because the cables are required to be connected.

NOTE: Precautions before the parts replacement
- When replacing GbE-4Port card, replace it with the instruction described in "Hitachi Advanced Server 8000/RS220xK Maintenance Manual" and confirm the operation after the replacement by using HATP (a program that executes operation confirmation and executes determination when a failure occurs on HA8000 series).
- Depend on the result of HATP, the other possible suspect parts might be replaced. In this case, return to 'C.2.2.1 Failure determination procedure at the cluster configuration' and determine the subject parts.
- Make sure to collect Simple log by using HATP before the replacement. For the details, refer to "Hitachi Advanced Server 8000/RS220xK Maintenance Manual."

(4) After replacing the GbE-4Port card, reconnect the cables where they were if they are all removed at the replacing procedure, and press the power button on the node.

NOTE:
- When there has been an instruction to let the heartbeat cable and maintenance port cable removed during operation before executing the replacement procedure, do not connect heartbeat cable and the maintenance port cable and just connect the other cables.
- Be sure to reconnect the LAN cables to the same ports as before.

(5) Confirm that the OS startup of the node is complete.
Refer to "Set Up '1.3 Startup Confirmation of the OS by using KVM' (SETUP 01-0010)" and confirm that the login prompt window is displayed.
If the login prompt window is not displayed and a boot failure window is displayed, the OS startup was not successful because another failure occurred. Refer to 'C.2.4 Diagnosis for OS Boot Failure' and execute the solution to the failure. After the failure is solved, proceed to the step (6).
If the login prompt window is displayed, proceed to the step (6).

Copyright © 2012, 2013, Hitachi, Ltd.

(6) Confirm the node status on the other side.
To check, execute the peerstatus command on the other (normal) node and check whether the status is [BOOT COMPLETE].
For details about how to check node status, refer to "Maintenance Tool '2.36 Displaying the Status of Other Side Node (peerstatus)' (MNTT 02-2130)".

NOTE: Wait approximately 10 minutes until the OS is completely started.

(7) After the OS is started, check the following.
Check the hardware status. Check whether "up" is displayed for the ports used in the new card in "Network Interface" on the screen. For details about how to check the hardware status, refer to 'B.3.1 Displaying the Hardware Status (hwstatus)'.

(8) Return to the step (e) of "Replacement '1.2.1 Parts replacement only when the node is turned off (cluster configuration)' (REP 01-0070)" and execute the rest of the procedures.

Copyright © 2012, 2013, Hitachi, Ltd.

D.1.7.2 Replacing the GbE-4Port Card (single node configuration)

(1) Stop the OS on the target node.
For details about how to stop the OS on a node, refer to "Maintenance Tool '2.28 Terminating the OS of This Side Node (nasshutdown)' (MNTT 02-1740)".

(2) Disconnect all the LAN cables from the GbE-4Port card.

(3) Refer to "Hitachi Advanced Server 8000/RS220xK Maintenance Manual" and replace the GbE-4Port card.
After the replacement, the power source must be stopped because the cables are required to be connected.

NOTE: Precautions before the parts replacement

- When replacing GbE-4Port card, replace it with the instruction described in "Hitachi Advanced Server 8000/RS220xK Maintenance Manual" and confirm the operation after the replacement by using HATP (a program that executes operation confirmation and executes determination when a failure occurs on HA8000 series).
- Depend on the result of HATP, the other possible suspect parts might be replaced. In this case, return to 'C.2.2.2 Failure determination procedure at the single node configuration' and determine the subject parts.
- Make sure to collect Simple log by using HATP before the replacement. For the details, refer to "Hitachi Advanced Server 8000/RS220xK Maintenance Manual."

(4) After replacing the GbE-4Port card, reconnect the cables where they were if they are all removed at the replacing procedure, and press the power button on the node.

NOTE:
- Be sure to reconnect the LAN cables to the same ports as before.

(5) Confirm that the OS startup of the node is complete.
Refer to "Set Up '1.3 Startup Confirmation of the OS by using KVM' (SETUP 01-0010)" and confirm that the login prompt window is displayed.
If the login prompt window is not displayed and a boot failure window is displayed, the OS startup was not successful because another failure occurred. Refer to 'C.2.4 Diagnosis for OS Boot Failure' and execute the solution to the failure. After the failure is solved, proceed to the step (6).
If the login prompt window is displayed, proceed to the step (6).

(6) Check if the resource group is running normally.
Execute rgstatus command to confirm whether the resource group is running normally.
For the method for confirmation, refer to "Maintenance Tool '2.63 Resource group Status Display (rgstatus)' (MNTT 02-3380)".

(7) After the OS is started, check the following.
- Check the hardware status. Check whether "up" is displayed for "eth0" and "eth1" status in "Network Interface" on the screen. For details about how to check the hardware status, refer to 'B.3.1 Displaying the Hardware Status (hwstatus)'.

(8) Return to the step (c) of "Replacement '1.2.2 Parts replacement only when the node is turned off (single node configuration)' (REP 01-0090)" and execute the rest of the procedures.

Copyright © 2012, 2013, Hitachi, Ltd.

D.1.8 Replacing the GbE-2Port Card

For the cluster configuration, refer to D.1.8.1 Replacing the GbE-2Port Card (cluster configuration).
For the single node configuration, refer to 'D.1.8.2 Replacing the GbE-2Port Card (single node configuration)'.

D.1.8.1 Replacing the GbE-2Port Card (cluster configuration)

(1) Stop the OS on the target node.
For details about how to stop the OS on a node, refer to "Maintenance Tool '2.28 Terminating the OS of This Side Node (nasshutdown)' (MNTT 02-1740)".

(2) Disconnect all the LAN cables from the GbE-2Port card.

(3) Refer to "Hitachi Advanced Server 8000/RS220xK Maintenance Manual" and replace the GbE-2Port card.
After the replacement, the power source must be stopped because the cables are required to be connected.

NOTE: Precautions before the parts replacement

- When replacing GbE-2Port card to be installed in the expansion slot 1, replace the standard bracket that attached to the maintenance part with the Low Profile bracket and screws that attached to the failure part.
- When replacing GbE-2Port card, replace it with the instruction described in "Hitachi Advanced Server 8000/RS220xK Maintenance Manual" and confirm the operation after the replacement by using HATP (a program that executes operation confirmation and executes determination when a failure occurs on HA8000 series).
- Depend on the result of HATP, the other possible suspect parts might be replaced. In this case, return to 'C.2.2.1 Failure determination procedure at the cluster configuration' and determine the subject parts.
- Make sure to collect Simple log by using HATP before the replacement. For the details, refer to "Hitachi Advanced Server 8000/RS220xK Maintenance Manual."

(4) After replacing the GbE-2Port card, reconnect the cables where they were if they are all removed at the replacing procedure, and press the power button on the node.

NOTE:
- When there has been an instruction to let the heartbeat cable and maintenance port cable removed during operation before executing the replacement procedure, do not connect heartbeat cable and the maintenance port cable and just connect the other cables.
- Be sure to reconnect the LAN cables to the same ports as before.

(5) Confirm that the OS startup of the node is complete.
Refer to "Set Up '1.3 Startup Confirmation of the OS by using KVM' (SETUP 01-0010)" and confirm that the login prompt window is displayed.
If the login prompt window is not displayed and a boot failure window is displayed, the OS startup was not successful because another failure occurred. Refer to 'C.2.4 Diagnosis for OS Boot Failure' and execute the solution to the failure. After the failure is solved, proceed to the step (6).
If the login prompt window is displayed, proceed to the step (6).

Copyright © 2012, 2013, Hitachi, Ltd.

(6) Confirm the node status on the other side.
To check, execute the peerstatus command on the other (normal) node and check whether the status is [BOOT COMPLETE].
For details about how to check node status, refer to "Maintenance Tool '2.36 Displaying the Status of Other Side Node (peerstatus)' (MNTT 02-2130)".

NOTE: Wait approximately 10 minutes until the OS is completely started.

(7) After the OS is started, check the following.
Check the hardware status. Check whether the status of "mng0" of "Network Interface" on the screen is displayed as "up".
For details about how to check the hardware status, refer to 'B.3.1 Displaying the Hardware Status (hwstatus)'.

(8) Return to the step (e) of "Replacement '1.2.1 Parts replacement only when the node is turned off (cluster configuration)' (REP 01-0070)" and execute the rest of the procedures.

Copyright © 2012, 2013, Hitachi, Ltd.

D.1.8.2 Replacing the GbE-2Port Card (single node configuration)

(1) Stop the OS on the target node. Before stopping the OS of the node, ask the system administrator if the service can be stopped or not. After that confirmation, execute the operation.
For details about how to stop the OS on a node, refer to "Maintenance Tool '2.28 Terminating the OS of This Side Node (nasshutdown)' (MNTT 02-1740)".

(2) Disconnect the LAN cables from the GbE-2Port card.

(3) Refer to "Hitachi Advanced Server 8000/RS220xK Maintenance Manual" and replace the GbE-2Port card. After the replacement, the power source must be stopped because the cables are required to be connected.

NOTE: Precautions before parts replacement

- When replacing GbE-2Port card to be installed in the expansion slot 1, replace the standard bracket that attached to the maintenance part with the Low Profile bracket and screws that attached to the failure part.
- When replacing GbE-2Port card, replace it with the instruction described in "Hitachi Advanced Server 8000/RS220xK Maintenance Manual" and confirm the operation after the replacement by using HATP (a program that executes operation confirmation and executes determination when a failure occurs on HA8000 series).
- Depend on the result of HATP, the other possible suspect parts might be replaced. In this case, return to 'C.2.2.2 Failure determination procedure at the single node configuration' and determine the subject parts.
- Make sure to collect Simple log by using HATP before the replacement. For the details, refer to "Hitachi Advanced Server 8000/RS220xK Maintenance Manual."

(4) After replacing the GbE-2Port card, reconnect the cables where they were if they are all removed at the replacing procedure, and press the power button on the node.

NOTE:
- Be sure to reconnect the LAN cables to the same ports as before.

(5) Confirm that the OS startup of the node is complete.
Refer to "Set Up '1.3 Startup Confirmation of the OS by using KVM' (SETUP 01-0010)" and confirm that the login prompt window is displayed.
If the login prompt window is not displayed and a boot failure window is displayed, the OS startup was not successful because another failure occurred. Refer to 'C.2.4 Diagnosis for OS Boot Failure' and execute the solution to the failure. After the failure is solved, proceed to the step (6).
If the login prompt window is displayed, proceed to the step (6).

NOTE: Wait approximately 10 minutes until the OS is completely started.

(6) Check if the resource group is running normally.
Execute rgstatus command to confirm whether the resource group is running normally.
For the method for confirmation, refer to "Maintenance Tool '2.63 Resource group Status Display (rgstatus)' (MNTT 02-3380)".

(7) After the OS is started, check the following.
Check the hardware status. Check that "up" is displayed for "eth0" and "eth1" in "Network Interface" on the screen. For details about how to check the hardware status, refer to 'B.3.1 Displaying the Hardware Status (hwstatus)'.

(8) Return to the step (c) of "Replacement '1.2.2 Parts replacement only when the node is turned off (single node configuration)' (REP 01-0090)" and execute the rest of the procedures.

Copyright © 2012, 2013, Hitachi, Ltd.

D.1.9 Replacing the Motherboard

For the cluster configuration, refer to D.1.9.1 Replacing the Motherboard (cluster configuration).
For the single node configuration, refer to 'D.1.9.2 Replacing the Motherboard (single node configuration)'.

D.1.9.1 Replacing the Motherboard (cluster configuration)

NOTE:
- Prior to the replacement of the motherboard stated in this section, a confirmation whether the SIM message (KAQG72026-E) for the forced failover has been output to the other side of the node or not, needs to be finished.
  If the confirmation has not been finished yet, check the SIM message on the other side of the node and also if the message "KAQG72026-E" has been output, execute 'C.2.2.1 Failure determination procedure at the cluster configuration' again. For the confirmation of SIM message, refer to "Maintenance Tool '2.6 Displaying SIMs on This Side (syseventlist)' (MNTT 02-0360)".
- BMC setting must be the same before the replacement of the motherboard because the communication might not be available if the different BMC setting is done.

(1) The replacement of the motherboard requires confirming and resetting the BMC. Therefore, confirm the BMC setting information, and write down the setting information. For the confirmation of the BMC setting, execute bmcctl command. If it is not available to log in to the node to be replaced, execute from the other side node. For more information about bmcctl command, refer to "Maintenance Tool '2.18 Setting BMC LAN Information (bmcctl)' (MNTT 02-1210)".

(2) Stop the OS on the target node.
For details about how to stop the OS on a node, refer to "Maintenance Tool '2.28 Terminating the OS of This Side Node (nasshutdown)' (MNTT 02-1740)".

(3) Disconnect all the cables connected to the node itself because the node is required to be replaced the parts at the support center. All those cables are reconnected after the node is returned. Therefore, be sure to write down the place to connect the cables.

(4) Remove HDD from the node.
The HDD is reinstalled after the node is returned. Therefore, be sure to write down the place to install the HDD.

(5) Explain the customer that the operation is done only by one side node because the other side node is required to be replaced the parts at the support center. And then intermittent the replacement operation.
When the confirmation of the returned node is complete, execute the following step.

(6) Check the place to connect the cables that are written down at the step (3), and reconnect all the cables to the node.

NOTE: When there has been an instruction to let the heartbeat cable and maintenance port cable removed during operation before executing the replacement procedure, do not connect heartbeat cable and the maintenance port cable and just connect the other cables.

(7) Check the place to install the HDD that is written down at the step (4), and re-install the HDD to the node.

(8) Refer to 'B.2.7 Confirmation of CPU Virtualization Support Mechanism' and confirm the virtualization support mechanism of the CPU.

Copyright © 2012, 2014, Hitachi, Ltd.

(9) Set the time of BIOS by any method of the following.

(a) Execute the timeget-u command in the node that has not been replaced, and set the displayed UTC time for BIOS. For the timeget command, refer to "Maintenance Tool '2.42 Acquisition of Time/Time Zone (timeget)' (MNTT 02-2430)".
For setting the BIOS time, refer to 'B.2.4 Set the Time in BIOS'.

(b) Refer to "Set Up '9.1 UTC-based Time Setting' (SETUP 09-0000)", and acquire the UTC time from the maintenance PC and set the time of BIOS.

(10) Confirm that the OS startup of the node is complete.
Refer to "Set Up '1.3 Startup Confirmation of the OS by using KVM' (SETUP 01-0010)" and confirm that the login prompt window is displayed.
If the login prompt window is not displayed and a boot failure window is displayed, the OS startup was not successful because another failure occurred. Refer to 'C.2.4 Diagnosis for OS Boot Failure' and execute the solution to the failure. After the failure is solved, proceed to the step (11).
If the login prompt window is displayed, proceed to the step (11).

(11) Set the account of BMC. For the setting of an account, refer to "Maintenance Tool '2.18 Setting BMC LAN Information (bmcctl)' (MNTT 02-1210)".

(12) Check the information of the BMC interface. Check if the information is not changed with the written information before replacing the motherboard.
If the information has been changed, set to the information as the written information before replacing the mother board again.
For the setting of the BMC interface information, refer to "Maintenance Tool '2.18 Setting BMC LAN Information (bmcctl)' (MNTT 02-1210)".

NOTE: If the operation instruction to remove heartbeat cable and management cable has been given in the Troubleshooting / Troubleshooting by each Model of this manual prior to the execution of the replacement procedure, confirmation and setting f the BMC interface information are not required. They will be executed in the Troubleshooting section.

(13) Execute the timeget command in the both node with no option specifying, and check that the present time matches in the both nodes. For the confirmation of the present time, make sure that the "Year, month, date, hour, and minute" are matched. For the present time confirmation, refer to "Maintenance Tool '2.18 Setting BMC LAN Information (bmcctl)' (MNTT 02-1210)".
If they are not matched, write down the present time on the node of not replaced, and set the time again with the timeset command for the node that executed the replacement. Rebooting is required after the time setting.
For the setting of the present time, refer to "Maintenance Tool '2.43 Time Setting (timeset)' (MNTT 02-2470)".

Copyright © 2012, 2014, Hitachi, Ltd.

(14) After completion of step (13), check the following.
Check the hardware statuses on the both nodes to confirm that both the “status” and “connection” of “BMC Information” in the window are “ok”. (For checking the hardware status, refer to ‘B.3.1 Displaying the Hardware Status (hwstatus)’.

NOTE: If under the recovery of the dual failure, confirm that the “status” in “BMC Information” of the motherboard replaced node shows “ok”.

If the operation instruction to remove heartbeat cable and management cable has been given in the Troubleshooting / Troubleshooting by each Model of this manual prior to the execution of the replacement procedure, return to the part replacement section of the Troubleshooting instead of proceeding to the step (15).

(15) Return to the step (e) of “Replacement ‘1.2.1 Parts replacement only when the node is turned off (cluster configuration)’ (REP 01-0070)”, and execute the rest of the procedures.

Copyright © 2011, 2013, Hitachi, Ltd.

D.1.9.2 Replacing the Motherboard (single node configuration)

(1) The replacement of the motherboard requires confirming and resetting the BMC. Therefore, confirm the BMC setting information, and write down the setting information. For the confirmation of the BMC setting, execute bmcctl command.
For more information about bmcctl command, refer to "Maintenance Tool '2.18 Setting BMC LAN Information (bmcctl)' (MNTT 02-1210)".

(2) Stop the OS on the target node.
For details about how to stop the OS on a node, refer to "Maintenance Tool '2.28 Terminating the OS of This Side Node (nasshutdown)' (MNTT 02-1740)".

(3) Disconnect all the cables connected to the node itself, because the node is required to be replaced the parts at the support center. All those cables are reconnected after the node is returned. Therefore, be sure to write down the place to connect the cables.

(4) Remove HDD from the node.
The HDD is reinstalled after the node is returned. Therefore, be sure to write down the place to install the HDD.

(5) Because the node is required to be replaced the parts at the support center, wait until the node is returned. When the node is returned, proceed to the next step.

(6) Connect all the cables to the node.

(7) Re-install the HDD.

(8) Refer to "Set Up '9.1 UTC-based Time Setting' (SETUP 09-0000)", and acquire the UTC time from the maintenance PC and set the time of BIOS.

(9) Confirm that the OS startup of the node is complete.
Refer to "Set Up '1.3 Startup Confirmation of the OS by using KVM' (SETUP 01-0010)" and confirm that the login prompt window is displayed.
If the login prompt window is not displayed and a boot failure window is displayed, the OS startup was not successful because another failure occurred. Refer to 'C.2.4 Diagnosis for OS Boot Failure' and execute the solution to the failure. After the failure is solved, proceed to the step (10).
If the login prompt window is displayed, proceed to the step (10).

NOTE: Wait approximately 10 minutes until the OS is completely started.

Copyright © 2012, 2013, Hitachi, Ltd.

(10) Check if the resource group is running normally.
Execute the rgstatus command to confirm whether the resource group is running normally. For the method for confirmation, refer to "Maintenance Tool '2.63 Resource group Status Display (rgstatus)' (MNTT 02-3380)".

(11) Check the information of the BMC interface. Check if the information is not changed with the written information before replacing the motherboard.
If the information has been changed, set to the information as the written information before replacing the mother board again.
For the setting of the BMC interface information, refer to "Maintenance Tool '2.18 Setting BMC LAN Information (bmcctl)' (MNTT 02-1210)".

(12) After completion of step (11), check the following.
Check the hardware statuses on the both nodes to confirm that both "status" of "BMC Information" in the window are "ok". (For checking the hardware status, refer to 'B.3.1 Displaying the Hardware Status (hwstatus)'.
If the OS version is 3.0.0-XX or later, proceed to step (13).
If the OS version is 2.2.0-XX or earlier, proceed to step (15).

(13) Check the set value for automatically relearn performing of the Internal RAID Battery.
However, this is not required in the configuration connected with the disk array subsystem.
If the OS version is 3.0.0-XX, execute bbuautolearnget command to confirm [Auto-Learn Mode] is [Enabled].
If the OS version is 3.0.1-XX or later, execute bburelearnget command to confirm "Status" is [Enable].
For the details about bbuautolearnget command, refer to "Maintenance Tool '2.68 Displaying the Set Value for Automatically Relearn Performing of the Internal RAID Battery (bbuautolearnget)' (MNTT 02-3650)".
For the details about bburelearnget command, refer to "Maintenance Tool "2.86 Displaying Relearn Schedule of Cache Backup Module and Setting Status (enabled/disabled) of Schedule Execution (bburelearnget)" (MNTT 02-4500)".

When [Auto-Learn Mode] is [Enabled] or "Status" is [Enable], proceed to step (15).
When [Auto-Learn Mode] is [Disabled] or "Status" is [Disable], proceed to step (14).

(14) Change the set value for automatically relearn performing of the Internal RAID Battery.
However, this is not required in the configuration connected with the disk array subsystem.
If the OS version is 3.0.0-XX, execute "bbuautolearnset --on" command and after that perform step (13) again.
If the OS version is 3.0.1-XX or later, execute "bburelearnset --enable" command and after that perform step (13) again.
For the details about bbuautolearnset command, refer to "Maintenance Tool '2.67 Setting for Automatically Relearn Performing of the Internal RAID Battery (bbuautolearnset)' (MNTT 02-3620)".
For the details about bburelearnset command, refer to "Maintenance Tool "2.87 Setting Relearn Schedule of Cache Backup Module and Enabling/disabling Schedule Execution (bburelearnset)" (MNTT 02-4530)".

(15) Collect the OS log of the node.
For the details about OS collection, refer to "Maintenance Tool '2.19 Collecting Logs (oslogget)' (MNTT 02-1300)".
If the OS version is 3.0.0-XX or later, proceed to step(16).
If the OS version is 2.2.0-XX or earlier, the replacement is complete by this step.

(16) Request the system administrator to check the cache writing mode setting when the battery level of the embedded RAID battery is low.
However, this is not required in the configuration connected with the disk array subsystem.

Copyright © 2012, 2014, Hitachi, Ltd.

D.1.10 Replacing the DVD Drive

For the cluster configuration, refer to D.1.10.1 Replacing the DVD Drive (cluster configuration).
For the single node configuration, refer to ‘D.1.10.2 Replacing the DVD Drive (single node configuration)’.

D.1.10.1 Replacing the DVD Drive (cluster configuration)

(1) Stop the OS on the target node.
For details about how to stop the OS on a node, refer to “Maintenance Tool ‘2.28 Terminating the OS of This Side Node (nasshutdown)’ (MNTT 02-1740)”.

(2) Refer to “HA8000/RS220xK Maintenance Manual” and replace the DVD drive.

NOTE: Precautions before the parts replacement
- When replacing DVD drive, replace it with the instruction described in “Hitachi Advanced Server 8000/RS220xK Maintenance Manual” and confirm the operation after the replacement by using HATP (a program that executes operation confirmation and executes determination when a failure occurs on HA8000 series).
- Depend on the result of HATP, the other possible suspect parts might be replaced. In this case, return to ‘C.2.2.1 Failure determination procedure at the cluster configuration’ and determine the subject parts.

(3) After replacing the DVD drive, reconnect the cables where they were if they are all removed at the replacing operation, and press the power button on the node.

NOTE: When there has been an instruction to let the heartbeat cable and maintenance port cable removed during operation before executing the replacement procedure, do not connect heartbeat cable and the maintenance port cable and just connect the other cables.

(4) Confirm that the OS startup of the node is complete.
Refer to “Set Up ‘1.3 Startup Confirmation of the OS by using KVM’ (SETUP 01-0010)” and confirm that the login prompt window is displayed.
If the login prompt window is not displayed and a boot failure window is displayed, the OS startup was not successful because another failure occurred. Refer to ‘C.2.4 Diagnosis for OS Boot Failure’ and execute the solution to the failure. After the failure is solved, proceed to the step (5).
If the login prompt window is displayed, proceed to the step (5).

(5) Check whether the OS is completely started on the node. To check, execute the peerstatus command on the other (normal) node and check whether the status is [BOOT COMPLETE].
For details about how to check node status, refer to “Maintenance Tool ‘2.36 Displaying the Status of Other Side Node (peerstatus)’ (MNTT 02-2130)”.

NOTE: Wait approximately 10 minutes until the OS is completely started.

(6) Return to the step (e) of “Replacement ‘1.2.1 Parts replacement only when the node is turned off (cluster configuration)’ (REP 01-0070)” and execute the rest of the procedures.

Copyright © 2012, 2013, Hitachi, Ltd.

D.1.10.2 Replacing the DVD Drive (single node configuration)

(1) Stop the OS on the target node.
Before stopping the OS of the node, ask the system administrator if the service can be stopped or not. After that confirmation, execute the operation.
For details about how to stop the OS on a node, refer to "Maintenance Tool '2.28 Terminating the OS of This Side Node (nasshutdown)' (MNTT 02-1740)".

(2) Refer to "HA8000/RS220xK Maintenance Manual" and replace the DVD drive.

NOTE: Precautions before the parts replacement

- When replacing DVD drive, replace it with the instruction described in "Hitachi Advanced Server 8000/RS220xK Maintenance Manual" and confirm the operation after the replacement by using HATP (a program that executes operation confirmation and executes determination when a failure occurs on HA8000 series).
- Depend on the result of HATP, the other possible suspect parts might be replaced. In this case, return to 'C.2.2.2 Failure determination procedure at the single node configuration' and determine the subject parts.

(3) After replacing the DVD drive, reconnect the cables where they were if they are all removed at the replacing operation, and press the power button on the node.

(4) Confirm that the OS startup of the node is complete.
Refer to "Set Up '1.3 Startup Confirmation of the OS by using KVM' (SETUP 01-0010)" and confirm that the login prompt window is displayed.
If the login prompt window is not displayed and a boot failure window is displayed, the OS startup was not successful because another failure occurred. Refer to 'C.2.4 Diagnosis for OS Boot Failure' and execute the solution to the failure. After the failure is solved, proceed to the step (5).
If the login prompt window is displayed, proceed to the step (5).

NOTE: Wait approximately 10 minutes until the OS is completely started.

(5) Check if the resource group is running normally.
Execute the rgstatus command to confirm whether the resource group is running normally. For the method for confirmation, refer to "Maintenance Tool '2.63 Resource group Status Display (rgstatus)' (MNTT 02-3380)".

(6) Return to the step (c) of "Replacement '1.2.2 Parts replacement only when the node is turned off (single node configuration)' (REP 01-0090)" and execute the rest of the procedures.

Copyright © 2012, 2013, Hitachi, Ltd.

D.1.11 Replacing the CPU

For the cluster configuration, refer to D.1.11.1 Replacing the CPU (cluster configuration).
For the single node configuration, refer to 'D.1.11.2 Replacing the CPU (single node configuration)'.

D.1.11.1 Replacing the CPU (cluster configuration)

(1) Stop the OS on the target node.
For details about how to stop the OS on a node, refer to "Maintenance Tool '2.28 Terminating the OS of This Side Node (nasshutdown)' (MNTT 02-1740)".

(2) Disconnect all the cables connected to the node itself, because the node is required to be replaced the parts at the support center. All those cables are reconnected after the node is returned. Therefore, be sure to write down the place to connect the cables.

(3) Remove HDD from the node.
The HDD is reinstalled after the node is returned. Therefore, be sure to write down the place to install the HDD.

(4) Because the node is required to be replaced the parts at the support center, wait until the node is returned. When the node is returned, proceed to the next step.

(5) Connect all the cables to the node.

NOTE: When there has been an instruction to let the heartbeat cable and maintenance port cable removed during operation before executing the replacement procedure, do not connect heartbeat cable and the maintenance port cable and just connect the other cables.

(6) Re-install the HDD and turn the Power lamp on.

(7) Confirm that the OS startup of the node is complete.
Refer to "Set Up '1.3 Startup Confirmation of the OS by using KVM' (SETUP 01-0010)" and confirm that the login prompt window is displayed.
If the login prompt window is not displayed and a boot failure window is displayed, the OS startup was not successful because another failure occurred. Refer to 'C.2.4 Diagnosis for OS Boot Failure' and execute the solution to the failure. After the failure is solved, proceed to the step (8).
If the login prompt window is displayed, proceed to the step (8).

NOTE: Wait approximately 10 minutes until the OS is completely started.

(8) Return to the step (e) of "Replacement '1.2.1 Parts replacement only when the node is turned off (cluster configuration)' (REP 01-0070)" and execute the rest of the procedures.

Copyright © 2012, 2013, Hitachi, Ltd.

D.1.11.2 Replacing the CPU (single node configuration)

(1) Stop the OS on the target node.
Before stopping the OS of the node, ask the system administrator if the service can be stopped or not. After that confirmation, execute the operation.
For details about how to stop the OS on a node, refer to "Maintenance Tool '2.28 Terminating the OS of This Side Node (nasshutdown)' (MNTT 02-1740)".

(2) Disconnect all the cables connected to the node itself, because the node is required to be replaced the parts at the support center. All those cables are reconnected after the node is returned. Therefore, be sure to write down the place to connect the cables.

(3) Remove HDD from the node.
The HDD is reinstalled after the node is returned. Therefore, be sure to write down the place to install the HDD.

(4) Because the node is required to be replaced the parts at the support center, wait until the node is returned. When the node is returned, proceed to the next step.

(5) Connect all the cables to the node.

(6) Re-install the HDD and turn the Power lamp on.

NOTE: Wait approximately 10 minutes until the OS is completely started.

(7) Confirm that the OS startup of the node is complete.
Refer to "Set Up '1.3 Startup Confirmation of the OS by using KVM' (SETUP 01-0010)" and confirm that the login prompt window is displayed.
If the login prompt window is not displayed and a boot failure window is displayed, the OS startup was not successful because another failure occurred. Refer to 'C.2.4 Diagnosis for OS Boot Failure' and execute the solution to the failure. After the failure is solved, proceed to the step (8).
If the login prompt window is displayed, proceed to the step (8).

(8) Check if the resource group is running normally.
Execute the rgstatus command to confirm whether the resource group is running normally. For the method for confirmation, refer to "Maintenance Tool '2.63 Resource group Status Display (rgstatus)' (MNTT 02-3380)".

(9) Return to the step (c) of "Replacement '1.2.2 Parts replacement only when the node is turned off (single node configuration)' (REP 01-0090)" and execute the rest of the procedures.

Copyright © 2012, 2013, Hitachi, Ltd.

D.1.12 Replacing the HDD Backplane Board

For the cluster configuration, refer to D.1.12.1 Replacing the HDD Backplane Board (cluster configuration).
For the single node configuration, refer to 'D.1.12.2 Replacing the HDD Backplane Board (single node configuration)'.

D.1.12.1 Replacing the HDD Backplane Board (cluster configuration)

(1) Stop the OS on the target node.
For details about how to stop the OS on a node, refer to "Maintenance Tool '2.28 Terminating the OS of This Side Node (nasshutdown)' (MNTT 02-1740)".

(2) Refer to "Hitachi Advanced Server 8000/RS220xK Maintenance Manual" and replace the HDD Backplane Board.

NOTE: Precautions before the parts replacement
- When replacing HDD Backplane Board, replace it with the instruction described in "Hitachi Advanced Server 8000/RS220xK Maintenance Manual" and confirm the operation after the replacement by using HATP (a program that executes operation confirmation and executes determination when a failure occurs on HA8000 series).
- Depend on the result of HATP, the other possible suspect parts might be replaced. In this case, return to 'C.2.2.1 Failure determination procedure at the cluster configuration' and determine the subject parts.

(3) After replacing the HDD Backplane Board, reconnect the cables where they were if they are all removed at the replacing operation, and press the power button on the node.

NOTE: When there has been an instruction to let the heartbeat cable and maintenance port cable removed during operation before executing the replacement procedure, do not connect heartbeat cable and the maintenance port cable and just connect the other cables.

(4) Confirm that the OS startup of the node is complete.
Refer to "Set Up '1.3 Startup Confirmation of the OS by using KVM' (SETUP 01-0010)" and confirm that the login prompt window is displayed.
If the login prompt window is not displayed and a boot failure window is displayed, the OS startup was not successful because another failure occurred. Refer to 'C.2.4 Diagnosis for OS Boot Failure' and execute the solution to the failure. After the failure is solved, proceed to the step (5).
If the login prompt window is displayed, proceed to the step (5).

(5) Confirm the node status on the other side.
To check, execute the peerstatus command on the other (normal) node and check whether the status is [BOOT COMPLETE].
For details about how to check node status, refer to "Maintenance Tool '2.36 Displaying the Status of Other Side Node (peerstatus)' (MNTT 02-2130)".

NOTE: Wait approximately 10 minutes until the OS is completely started.

Copyright © 2012, 2013, Hitachi, Ltd.

(6) After the OS is started, check the following.
Check the hardware status. Check whether “ok” is displayed for the status of 0 and 1 of “InternalHDD Information” on the screen. For details about how to check the hardware status, refer to ‘B.3.1 Displaying the Hardware Status (hwstatus)’.

(7) Return to the step (e) of “Replacement ‘1.2.1 Parts replacement only when the node is turned off (cluster configuration)’ (REP 01-0070)” and execute the rest of the procedures.

Copyright © 2011, 2013, Hitachi, Ltd.

D.1.12.2 Replacing the HDD Backplane Board (single node configuration)

(1) Stop the OS on the target node.
Before stopping the OS of the node, ask the system administrator if the service can be stopped or not. After that confirmation, execute the operation.
For details about how to stop the OS on a node, refer to "Maintenance Tool '2.28 Terminating the OS of This Side Node (nasshutdown)' (MNTT 02-1740)".

(2) Refer to "Hitachi Advanced Server 8000/RS220xK Maintenance Manual" and replace the HDD Backplane Board.

NOTE: Precautions before the parts replacement

- When replacing HDD Backplane Board, replace it with the instruction described in "Hitachi Advanced Server 8000/RS220xK Maintenance Manual" and confirm the operation after the replacement by using HATP (a program that executes operation confirmation and executes determination when a failure occurs on HA8000 series).
- Depend on the result of HATP, the other possible suspect parts might be replaced. In this case, return to 'C.2.2.2 Failure determination procedure at the single node configuration' and determine the subject parts.

(3) After replacing the HDD Backplane Board, reconnect the cables where they were if they are all removed at the replacing operation, and press the power button on the node.

(4) Confirm that the OS startup of the node is complete.
Refer to "Set Up '1.3 Startup Confirmation of the OS by using KVM' (SETUP 01-0010)" and confirm that the login prompt window is displayed.
If the login prompt window is not displayed and a boot failure window is displayed, the OS startup was not successful because another failure occurred. Refer to 'C.2.4 Diagnosis for OS Boot Failure' and execute the solution to the failure. After the failure is solved, proceed to the step (5).
If the login prompt window is displayed, proceed to the step (5).

NOTE: Wait approximately 10 minutes until the OS is completely started.

(5) Check if the resource group is running normally.
Execute rgstatus command to confirm whether the resource group is running normally.
For the method for confirmation, refer to "Maintenance Tool '2.63 Resource group Status Display (rgstatus)' (MNTT 02-3380)".

Copyright © 2012, 2013, Hitachi, Ltd.

(6) Check the hardware status.
Check the hardware status. Check whether “ok” is displayed for both 0 and 1 of “InternalHDD Information” on the screen.
For details about how to check the hardware status, refer to ‘B.3.1 Displaying the Hardware Status (hwstatus)’.

(7) Return to the step (c) of “Replacement ‘1.2.2 Parts replacement only when the node is turned off (single node configuration)’ (REP 01-0090)” and execute the rest of the procedures.

Copyright © 2012, 2013, Hitachi, Ltd.

D.1.13 Replacing the Front Panel Board

For the cluster configuration, refer to D.1.13.1 Replacing the Front Panel Board (cluster configuration).
For the single node configuration, refer to 'D.1.13.2 Replacing the Front Panel Board (single node configuration)'.

D.1.13.1 Replacing the Front Panel Board (cluster configuration)

(1) Stop the OS on the target node.
For details about how to stop the OS on a node, refer to "Maintenance Tool '2.28 Terminating the OS of This Side Node (nasshutdown)' (MNTT 02-1740)".

(2) Disconnect all the cables connected to the node itself, because the node is required to be replaced the parts at the support center. All those cables are reconnected after the node is returned. Therefore, be sure to write down the place to connect the cables.

(3) Remove HDD from the node.
The HDD is reinstalled after the node is returned. Therefore, be sure to write down the place to install the HDD.

(4) Because the node is required to be replaced the parts at the support center, wait until the node is returned. When the node is returned, proceed to the next step.

(5) Connect all the cables to the node.

NOTE: When there has been an instruction to let the heartbeat cable and maintenance port cable removed during operation before executing the replacement procedure, do not connect heartbeat cable and the maintenance port cable and just connect the other cables.

(6) Re-install the HDD and turn the Power lamp on.

(7) Confirm that the OS startup of the node is complete.
Refer to "Set Up '1.3 Startup Confirmation of the OS by using KVM' (SETUP 01-0010)" and confirm that the login prompt window is displayed.
If the login prompt window is not displayed and a boot failure window is displayed, the OS startup was not successful because another failure occurred. Refer to 'C.2.4 Diagnosis for OS Boot Failure' and execute the solution to the failure. After the failure is solved, proceed to the step (5).
If the login prompt window is displayed, proceed to the step (5).

(8) Confirm the node status on the other side.
To check, execute the peerstatus command on the other (normal) node and check whether the status is [BOOT COMPLETE].
For details about how to check node status, refer to "Maintenance Tool '2.36 Displaying the Status of Other Side Node (peerstatus)' (MNTT 02-2130)".

NOTE: Wait approximately 10 minutes until the OS is completely started.

(9) Return to the step (e) of "Replacement '1.2.1 Parts replacement only when the node is turned off (cluster configuration)' (REP 01-0070)" and execute the rest of the procedures.

Copyright © 2012, 2013, Hitachi, Ltd.

D.1.13.2 Replacing the Front Panel Board (single node configuration)

(1) Stop the OS on the target node.
Before stopping the OS of the node, ask the system administrator if the service can be stopped or not. After that confirmation, execute the operation.
For details about how to stop the OS on a node, refer to "Maintenance Tool '2.28 Terminating the OS of This Side Node (nasshutdown)' (MNTT 02-1740)".

(2) Disconnect all the cables connected to the node itself, because the node is required to be replaced the parts at the support center. All those cables are reconnected after the node is returned. Therefore, be sure to write down the place to connect the cables.

(3) Remove HDD from the node.
The HDD is reinstalled after the node is returned. Therefore, be sure to write down the place to install the HDD.

(4) Because the node is required to be replaced the parts at the support center, wait until the node is returned. When the node is returned, proceed to the next step.

(5) Connect all the cables to the node.

(6) Re-install the HDD and turn the Power lamp on.

(7) Confirm that the OS startup of the node is complete.
Refer to "Set Up '1.3 Startup Confirmation of the OS by using KVM' (SETUP 01-0010)" and confirm that the login prompt window is displayed.
If the login prompt window is not displayed and a boot failure window is displayed, the OS startup was not successful because another failure occurred. Refer to 'C.2.4 Diagnosis for OS Boot Failure' and execute the solution to the failure. After the failure is solved, proceed to the step (8).
If the login prompt window is displayed, proceed to the step (8).

NOTE: Wait approximately 10 minutes until the OS is completely started.

(8) Check if the resource group is running normally.
Execute the rgstatus command to confirm whether the resource group is running normally. For the method for confirmation, refer to "Maintenance Tool '2.63 Resource group Status Display (rgstatus)' (MNTT 02-3380)".

(9) Return to the step (c) of "Replacement '1.2.2 Parts replacement only when the node is turned off (single node configuration)' (REP 01-0090)" and execute the rest of the procedures.

Copyright © 2012, 2013, Hitachi, Ltd.

D.1.14 Replacing the PS Backboard

For the cluster configuration, refer to D.1.14.1 Replacing the PS Backboard (cluster configuration).
For the single node configuration, refer to 'D.1.14.2 Replacing the PS Backboard (single node configuration)'.

D.1.14.1 Replacing the PS Backboard (cluster configuration)

(1) Stop the OS on the target node.
For details about how to stop the OS on a node, refer to "Maintenance Tool '2.28 Terminating the OS of This Side Node (nasshutdown)' (MNTT 02-1740)".

(2) Refer to "Hitachi Advanced Server 8000/RS220xK Maintenance Manual" and replace the PS Backboard.

NOTE: Precautions before the parts replacement
- When replacing PS Backboard, replace it with the instruction described in "Hitachi Advanced Server 8000/RS220xK Maintenance Manual" and confirm the operation after the replacement by using HATP (a program that executes operation confirmation and executes determination when a failure occurs on HA8000 series).
- Depend on the result of HATP, the other possible suspect parts might be replaced. In this case, return to 'C.2.2.1 Failure determination procedure at the cluster configuration' and determine the subject parts.

(3) After replacing the PS Backboard, reconnect the cables where they were if they are all removed at the replacing operation, and press the power button on the node.

NOTE: When there has been an instruction to let the heartbeat cable and maintenance port cable removed during operation before executing the replacement procedure, do not connect heartbeat cable and the maintenance port cable and just connect the other cables.

(4) Confirm that the OS startup of the node is complete.
Refer to "Set Up '1.3 Startup Confirmation of the OS by using KVM' (SETUP 01-0010)" and confirm that the login prompt window is displayed.
If the login prompt window is not displayed and a boot failure window is displayed, the OS startup was not successful because another failure occurred. Refer to 'C.2.4 Diagnosis for OS Boot Failure' and execute the solution to the failure. After the failure is solved, proceed to the step (5).
If the login prompt window is displayed, proceed to the step (5).

(5) Check whether the OS is completely started on the node. To check, execute the peerstatus command on the other (normal) node and check whether the status is [BOOT COMPLETE].
For details about how to check node status, refer to "Maintenance Tool '2.36 Displaying the Status of Other Side Node (peerstatus)' (MNTT 02-2130)".

NOTE: Wait approximately 10 minutes until the OS is completely started.

Copyright © 2012, 2013, Hitachi, Ltd.

(6) After the OS is started, check the following.
Check the hardware status. Check whether “ok” is displayed for the status of 0 and 1 of “Power Supply Information” on the screen. For details about how to check the hardware status, refer to ‘B.3.1 Displaying the Hardware Status (hwstatus)’.

(7) Return to the step (e) of “Replacement ‘1.2.1 Parts replacement only when the node is turned off (cluster configuration)’ (REP 01-0070)” and execute the rest of the procedures.

Copyright © 2011, 2015, Hitachi, Ltd.

D.1.14.2 Replacing the PS Backboard (single node configuration)

(1) Stop the OS on the target node.
For details about how to stop the OS on a node, refer to "Maintenance Tool '2.28 Terminating the OS of This Side Node (nasshutdown)' (MNTT 02-1740)".

(2) Refer to "Hitachi Advanced Server 8000/RS220xK Maintenance Manual" and replace the PS Backboard.

NOTE: Precautions before the parts replacement

- When replacing PS Backboard, replace it with the instruction described in "Hitachi Advanced Server 8000/RS220xK Maintenance Manual" and confirm the operation after the replacement by using HATP (a program that executes operation confirmation and executes determination when a failure occurs on HA8000 series).
- Depend on the result of HATP, the other possible suspect parts might be replaced. In this case, return to 'C.2.2.2 Failure determination procedure at the single node configuration' and determine the subject parts.

(3) After replacing the PS Backboard, reconnect the cables where they were if they are all removed at the replacing operation, and press the power button on the node.

(4) Confirm that the OS startup of the node is complete.
Refer to "Set Up '1.3 Startup Confirmation of the OS by using KVM' (SETUP 01-0010)" and confirm that the login prompt window is displayed.
If the login prompt window is not displayed and a boot failure window is displayed, the OS startup was not successful because another failure occurred. Refer to 'C.2.4 Diagnosis for OS Boot Failure' and execute the solution to the failure. After the failure is solved, proceed to the step (5).
If the login prompt window is displayed, proceed to the step (5).

NOTE: Wait approximately 10 minutes until the OS is completely started.

(5) Check if the resource group is running normally.
Execute the rgstatus command to confirm whether the resource group is running normally. For the method for confirmation, refer to "Maintenance Tool '2.63 Resource group Status Display (rgstatus)' (MNTT 02-3380)".

(6) After the OS is started, check the following.
Check the hardware status. Check whether "ok" is displayed for both 0 and 1 of "Power Supply Information" on the screen. For details about how to check the hardware status, refer to 'B.3.1 Displaying the Hardware Status (hwstatus)'.

(7) Return to the step (c) of "Replacement '1.2.2 Parts replacement only when the node is turned off (single node configuration)' (REP 01-0090)" and execute the rest of the procedures.

Copyright © 2012, 2016, Hitachi, Ltd.

D.1.15 Replacing the Lithium Battery

For the cluster configuration, refer to D.1.15.1 Replacing the Lithium Battery (cluster configuration).
For the single node configuration, refer to ‘D.1.15.2 Replacing the Lithium Battery (single node configuration)’.

D.1.15.1 Replacing the Lithium Battery (cluster configuration)

(1) Stop the OS on the target node.
For details about how to stop the OS on a node, refer to “Maintenance Tool ‘2.28 Terminating the OS of This Side Node (nasshutdown)’ (MNTT 02-1740)”.

(2) Refer to “HA8000/RS220xK Maintenance Manual” and replace the Lithium Battery.

NOTE: Precautions before the parts replacement

- When replacing Lithium Battery, replace it with the instruction described in “Hitachi Advanced Server 8000/RS220xK Maintenance Manual” and confirm the operation after the replacement by using HATP (a program that executes operation confirmation and executes determination when a failure occurs on HA8000 series).
- Depend on the result of HATP, the other possible suspect parts might be replaced. In this case, return to ‘C.2.2.1 Failure determination procedure at the cluster configuration’ and determine the subject parts.
- Make sure to collect Simple log by using HATP before the replacement. For the details, refer to “Hitachi Advanced Server 8000/RS220xK Maintenance Manual.”

(3) After replacing the Lithium Battery, reconnect the cables where they were if they are all removed at the replacing operation, and press the power button on the node.

NOTE: When there has been an instruction to let the heartbeat cable and maintenance port cable removed during operation before executing the replacement procedure, do not connect heartbeat cable and the maintenance port cable and just connect the other cables.

(3-1) Refer to ‘B.2.7 Confirmation of CPU Virtualization Support Mechanism’ and verify CPU virtualization support mechanism.

(4) Confirm that the OS startup of the node is complete.
Refer to “Set Up ‘1.3 Startup Confirmation of the OS by using KVM’ (SETUP 01-0010)” and confirm that the login prompt window is displayed.
If the login prompt window is not displayed and a boot failure window is displayed, the OS startup was not successful because another failure occurred. Refer to ‘C.2.4 Diagnosis for OS Boot Failure’ and execute the solution to the failure. After the failure is solved, proceed to the step (5).
If the login prompt window is displayed, proceed to the step (5).

(5) Confirm the node status on the other side.
To check, execute the peerstatus command on the other (normal) node and check whether the status is [BOOT COMPLETE].
For details about how to check node status, refer to “Maintenance Tool ‘2.36 Displaying the Status of Other Side Node (peerstatus)’ (MNTT 02-2130)”.

NOTE: Wait approximately 10 minutes until the OS is completely started.

Copyright © 2012, 2013, Hitachi, Ltd.

(6) Confirm the time of the node.
Execute the timeget command in the both node with no option specifying, and check that the present time matches in the both nodes. For the confirmation of the present time, make sure that the "Year, month, date, hour, and minute" are matched. For the present time confirmation, refer to "Maintenance Tool '2.42 Acquisition of Time/ Time Zone (timeget)' (MNTT 02-2430)".
If they are not matched, write down the present time on the node of not replaced, and set the time again with the timeset command for the node that executed the replacement. Rebooting is required after the time setting. For the setting of the present time, refer to "Maintenance Tool '2.43 Time Setting (timeset)' (MNTT 02-2470)".

(7) Return to the step (e) of "Replacement '1.2.1 Parts replacement only when the node is turned off (cluster configuration)' (REP 01-0070)" and execute the rest of the procedures.

Copyright © 2011, 2013, Hitachi, Ltd.

D.1.15.2 Replacing the Lithium Battery (single node configuration)

(1) Stop the OS on the target node.
Before stopping the OS of the node, ask the system administrator if the service can be stopped or not. After that confirmation, execute the operation.
For details about how to stop the OS on a node, refer to "Maintenance Tool '2.28 Terminating the OS of This Side Node (nasshutdown)' (MNTT 02-1740)".

(2) Refer to "HA8000/RS220xK Maintenance Manual" and replace the Lithium Battery.

NOTE: Precautions before the parts replacement

- When replacing Lithium Battery, replace it with the instruction described in "Hitachi Advanced Server 8000/RS220xK Maintenance Manual" and confirm the operation after the replacement by using HATP (a program that executes operation confirmation and executes determination when a failure occurs on HA8000 series).
- Depend on the result of HATP, the other possible suspect parts might be replaced. In this case, return to 'C.2.2.2 Failure determination procedure at the single node configuration' and determine the subject parts.
- Make sure to collect Simple log by using HATP before the replacement. For the details, refer to "Hitachi Advanced Server 8000/RS220xK Maintenance Manual."

(3) After replacing the Lithium Battery, reconnect the cables where they were if they are all removed at the replacing operation, and press the power button on the node.

(4) Confirm that the OS startup of the node is complete.
Refer to "Set Up '1.3 Startup Confirmation of the OS by using KVM' (SETUP 01-0010)" and confirm that the login prompt window is displayed.
If the login prompt window is not displayed and a boot failure window is displayed, the OS startup was not successful because another failure occurred. Refer to 'C.2.4 Diagnosis for OS Boot Failure' and execute the solution to the failure. After the failure is solved, proceed to the step (5).
If the login prompt window is displayed, proceed to the step (5).

NOTE: Wait approximately 10 minutes until the OS is completely started.

(5) Check if the resource group is running normally.
Execute the rgstatus command to confirm whether the resource group is running normally. For the method for confirmation, refer to "Maintenance Tool '2.63 Resource group Status Display (rgstatus)' (MNTT 02-3380)".

(6) Confirm the time of the node.
Refer to "Set Up '9.1 UTC-based Time Setting' (SETUP 09-0000)", acquire the UTC time from the maintenance PC and set the time of BIOS.

(7) Return to the step (c) of "Replacement '1.2.2 Parts replacement only when the node is turned off (single node configuration)' (REP 01-0090)" and execute the rest of the procedures.

Copyright © 2012, 2013, Hitachi, Ltd.

D.1.16 Replacing the PCI Riser Board

For the cluster configuration, refer to D.1.16.1 Replacing the Lithium Battery (cluster configuration).
For the single node configuration, refer to 'D.1.16.2 Replacing the PCI Riser Board (single node configuration)'.

D.1.16.1 Replacing the PCI Riser Board (cluster configuration)

(1) Stop the OS on the target node.
For details about how to stop the OS on a node, refer to "Maintenance Tool '2.28 Terminating the OS of This Side Node (nasshutdown)' (MNTT 02-1740)".

(2) Refer to "Hitachi Advanced Server 8000/RS220xK Maintenance Manual" and replace the PCI Riser Board.

NOTE: Precautions before the parts replacement

- When replacing PCI Riser Board, replace it with the instruction described in "Hitachi Advanced Server 8000/RS220xK Maintenance Manual" and confirm the operation after the replacement by using HATP (a program that executes operation confirmation and executes determination when a failure occurs on HA8000 series).
- There are two kinds in the PCI Riser Board, PCI Riser A Board and PCI Riser B Board. For which PCI Riser Board is the target to be replaced, follow the instruction of "Hitachi Advanced Server 8000/RS220xK Maintenance Manual".
- Depend on the result of HATP, the other possible suspect parts might be replaced. In this case, return to 'C.2.2.1 Failure determination procedure at the cluster configuration' and determine the subject parts.
- Make sure to collect Simple log by using HATP before the replacement. For the details, refer to "Hitachi Advanced Server 8000/RS220xK Maintenance Manual."

(3) After replacing the PCI Riser Board, reconnect the cables where they were if they are all removed at the replacing operation, and press the power button on the node.

NOTE: When there has been an instruction to let the heartbeat cable and maintenance port cable removed during operation before executing the replacement procedure, do not connect heartbeat cable and the maintenance port cable and just connect the other cables.

Copyright © 2012, 2013, Hitachi, Ltd.

(4) Confirm that the OS startup of the node is complete.
Refer to "Set Up '1.3 Startup Confirmation of the OS by using KVM' (SETUP 01-0010)" and confirm that the login prompt window is displayed.
If the login prompt window is not displayed and a boot failure window is displayed, the OS startup was not successful because another failure occurred. Refer to 'C.2.4 Diagnosis for OS Boot Failure' and execute the solution to the failure. After the failure is solved, proceed to the step (5).
If the login prompt window is displayed, proceed to the step (5).

(5) Confirm the node status on the other side.
To check, execute the peerstatus command on the other (normal) node and check whether the status is [BOOT COMPLETE].
For details about how to check node status, refer to "Maintenance Tool '2.36 Displaying the Status of Other Side Node (peerstatus)' (MNTT 02-2130)".

NOTE: Wait approximately 10 minutes until the OS is completely started.

(6) Return to the step (e) of "Replacement '1.2.1 Parts replacement only when the node is turned off (cluster configuration)' (REP 01-0070)" and execute the rest of the procedures.

Copyright © 2012, 2013, Hitachi, Ltd.

D.1.16.2 Replacing the PCI Riser Board (single node configuration)

(1) Stop the OS on the target node.
For details about how to stop the OS on a node, refer to "Maintenance Tool '2.28 Terminating the OS of This Side Node (nasshutdown)' (MNTT 02-1740)".

(2) Refer to "Hitachi Advanced Server 8000/RS220xK Maintenance Manual" and replace the PCI Riser Board.

NOTE: Precautions before the parts replacement

- When replacing PCI Riser Board, replace it with the instruction described in "Hitachi Advanced Server 8000/RS220xK Maintenance Manual" and confirm the operation after the replacement by using HATP (a program that executes operation confirmation and executes determination when a failure occurs on HA8000 series).
- There are two kinds in the PCI Riser Board, PCI Riser A Board and PCI Riser B Board. For which PCI Riser Board is the target to be replaced, follow the instruction of "Hitachi Advanced Server 8000/RS220xK Maintenance Manual".
- Depend on the result of HATP, the other possible suspect parts might be replaced. In this case, return to 'C.2.2.2 Failure determination procedure at the single node configuration' and determine the subject parts.
- Make sure to collect Simple log by using HATP before the replacement. For the details, refer to "Hitachi Advanced Server 8000/RS220xK Maintenance Manual."

(3) After replacing the PCI Riser Board, reconnect the cables where they were if they are all removed at the replacing operation, and press the power button on the node.

(4) Confirm that the OS startup of the node is complete.
Refer to "Set Up '1.3 Startup Confirmation of the OS by using KVM' (SETUP 01-0010)" and confirm that the login prompt window is displayed.
If the login prompt window is not displayed and a boot failure window is displayed, the OS startup was not successful because another failure occurred. Refer to 'C.2.4 Diagnosis for OS Boot Failure' and execute the solution to the failure. After the failure is solved, proceed to the step (5).
If the login prompt window is displayed, proceed to the step (5).

NOTE: Wait approximately 10 minutes until the OS is completely started.

(5) Check if the resource group is running normally.
Execute the rgstatus command to confirm whether the resource group is running normally. For the method for confirmation, refer to "Maintenance Tool '2.63 Resource group Status Display (rgstatus)' (MNTT 02-3380)".

(6) Return to the step (c) of "Replacement '1.2.2 Parts replacement only when the node is turned off (single node configuration)' (REP 01-0090)" and execute the rest of the procedures.

Copyright © 2012, 2013, Hitachi, Ltd.

D.1.17 Replacing the CPU Heatsink

For the cluster configuration, refer to D.1.17.1 Replacing the CPU Heatsink (cluster configuration).
For the single node configuration, refer to 'D.1.17.2 Replacing the CPU Heatsink (single node configuration)'.

D.1.17.1 Replacing the CPU Heatsink (cluster configuration)

(1) Stop the OS on the target node.
For details about how to stop the OS on a node, refer to "Maintenance Tool '2.28 Terminating the OS of This Side Node (nasshutdown)' (MNTT 02-1740)".

(2) Disconnect all the cables connected to the node itself, because the node is required to be replaced the parts at the support center. All those cables are reconnected after the node is returned. Therefore, be sure to write down the place to connect the cables.

(3) Remove HDD from the node.
The HDD is reinstalled after the node is returned. Therefore, be sure to write down the place to install the HDD.

(4) Because the node is required to be replaced the parts at the support center, wait until the node is returned. When the node is returned, proceed to the next step.

(5) Connect all the cables to the node.

NOTE: When there has been an instruction to let the heartbeat cable and maintenance port cable removed during operation before executing the replacement procedure, do not connect heartbeat cable and the maintenance port cable and just connect the other cables.

(6) Re-install the HDD and turn the Power lamp on.

(7) Confirm that the OS startup of the node is complete.
Refer to "Set Up '1.3 Startup Confirmation of the OS by using KVM' (SETUP 01-0010)" and confirm that the login prompt window is displayed.
If the login prompt window is not displayed and a boot failure window is displayed, the OS startup was not successful because another failure occurred. Refer to 'C.2.4 Diagnosis for OS Boot Failure' and execute the solution to the failure. After the failure is solved, proceed to the step (8).
If the login prompt window is displayed, proceed to the step (8).

(8) Check whether the OS is completely started on the node. To check, execute the peerstatus command on the other (normal) node and check whether the status is [BOOT COMPLETE].
For details about how to check node status, refer to "Maintenance Tool '2.36 Displaying the Status of Other Side Node (peerstatus)' (MNTT 02-2130)".

NOTE: Wait approximately 10 minutes until the OS is completely started.

(9) Return to the step (e) of "Replacement '1.2.1 Parts replacement only when the node is turned off (cluster configuration)' (REP 01-0070)" and execute the rest of the procedures.

Copyright © 2012, 2013, Hitachi, Ltd.

D.1.17.2 Replacing the CPU Heatsink (single node configuration)

(1) Stop the OS on the target node.
Before stopping the OS of the node, ask the system administrator if the service can be stopped or not. After that confirmation, execute the operation.
For details about how to stop the OS on a node, refer to "Maintenance Tool '2.28 Terminating the OS of This Side Node (nasshutdown)' (MNTT 02-1740)".

(2) Disconnect all the cables connected to the node itself, because the node is required to be replaced the parts at the support center. All those cables are reconnected after the node is returned. Therefore, be sure to write down the place to connect the cables.

(3) Remove HDD from the node.
The HDD is reinstalled after the node is returned. Therefore, be sure to write down the place to install the HDD.

(4) Because the node is required to be replaced the parts at the support center, wait until the node is returned. When the node is returned, proceed to the next step.

(5) Connect all the cables to the node.

(6) Re-install the HDD and turn the Power lamp on.

(7) Confirm that the OS startup of the node is complete.
Refer to "Set Up '1.3 Startup Confirmation of the OS by using KVM' (SETUP 01-0010)" and confirm that the login prompt window is displayed.
If the login prompt window is not displayed and a boot failure window is displayed, the OS startup was not successful because another failure occurred. Refer to 'C.2.4 Diagnosis for OS Boot Failure' and execute the solution to the failure. After the failure is solved, proceed to the step (5).
If the login prompt window is displayed, proceed to the step (5).

NOTE: Wait approximately 10 minutes until the OS is completely started.

(8) Check if the resource group is running normally.
Execute the rgstatus command to confirm whether the resource group is running normally. For the method for confirmation, refer to "Maintenance Tool '2.63 Resource group Status Display (rgstatus)' (MNTT 02-3380)".

(9) Return to the step (c) of "Replacement '1.2.2 Parts replacement only when the node is turned off (single node configuration)' (REP 01-0090)" and execute the rest of the procedures.

Copyright © 2012, 2013, Hitachi, Ltd.

D.1.18 Replacing the CPU Air Duct

For the cluster configuration, refer to D.1.18.1 Replacing the CPU Air Duct (cluster configuration).
For the single node configuration, refer to 'D.1.18.2 Replacing the CPU Air Duct (single node configuration)'.

D.1.18.1 Replacing the CPU Air Duct (cluster configuration)

(1) Stop the OS on the target node.
For details about how to stop the OS on a node, refer to "Maintenance Tool '2.28 Terminating the OS of This Side Node (nasshutdown)' (MNTT 02-1740)".

(2) Refer to "Hitachi Advanced Server 8000/RS220xK Maintenance Manual" and replace the CPU Air Duct.

NOTE: Precautions before the parts replacement
- When replacing CPU Air Duct, replace it with the instruction described in "Hitachi Advanced Server 8000/RS220xK Maintenance Manual" and confirm the operation after the replacement by using HATP (a program that executes operation confirmation and executes determination when a failure occurs on HA8000 series).
- Depend on the result of HATP, the other possible suspect parts might be replaced. In this case, return to 'C.2.2.1 Failure determination procedure at the cluster configuration' and determine the subject parts.

(3) After replacing the CPU Air Duct, reconnect the cables where they were if they are all removed at the replacing operation, and press the power button on the node.

NOTE: When there has been an instruction to let the heartbeat cable and maintenance port cable removed during operation before executing the replacement procedure, do not connect heartbeat cable and the maintenance port cable and just connect the other cables.

(4) Confirm that the OS startup of the node is complete.
Refer to "Set Up '1.3 Startup Confirmation of the OS by using KVM' (SETUP 01-0010)" and confirm that the login prompt window is displayed. If the login prompt window is not displayed and a boot failure window is displayed, the OS startup was not successful because another failure occurred. Refer to 'C.2.4 Diagnosis for OS Boot Failure' and execute the solution to the failure. After the failure is solved, proceed to the step (5).
If the login prompt window is displayed, proceed to the step (5).

(5) Check whether the OS is completely started on the node. To check, execute the peerstatus command on the other (normal) node and check whether the status is [BOOT COMPLETE].
For details about how to check node status, refer to "Maintenance Tool '2.36 Displaying the Status of Other Side Node (peerstatus)' (MNTT 02-2130)".

NOTE: Wait approximately 10 minutes until the OS is completely started.

(6) Return to the step (e) of "Replacement '1.2.1 Parts replacement only when the node is turned off (cluster configuration)' (REP 01-0070)" and execute the rest of the procedures.

Copyright © 2012, 2013, Hitachi, Ltd.

D.1.18.2 Replacing the CPU Air Duct (single node configuration)

(1) Stop the OS on the target node.
Before stopping the OS of the node, ask the system administrator if the service can be stopped or not. After that confirmation, execute the operation.
For details about how to stop the OS on a node, refer to "Maintenance Tool '2.28 Terminating the OS of This Side Node (nasshutdown)' (MNTT 02-1740)".

(2) Refer to "Hitachi Advanced Server 8000/RS220xK Maintenance Manual" and replace the CPU Air Duct.

NOTE: Precautions before the parts replacement

- When replacing CPU Air Duct, replace it with the instruction described in "Hitachi Advanced Server 8000/RS220xK Maintenance Manual" and confirm the operation after the replacement by using HATP (a program that executes operation confirmation and executes determination when a failure occurs on HA8000 series).
- Depend on the result of HATP, the other possible suspect parts might be replaced. In this case, return to 'C.2.2.2 Failure determination procedure at the single node configuration' and determine the subject parts.

(3) After replacing the CPU Air Duct, reconnect the cables where they were if they are all removed at the replacing operation, and press the power button on the node.

(4) Confirm that the OS startup of the node is complete.
Refer to "Set Up '1.3 Startup Confirmation of the OS by using KVM' (SETUP 01-0010)" and confirm that the login prompt window is displayed.
If the login prompt window is not displayed and a boot failure window is displayed, the OS startup was not successful because another failure occurred. Refer to 'C.2.4 Diagnosis for OS Boot Failure' and execute the solution to the failure. After the failure is solved, proceed to the step (5).
If the login prompt window is displayed, proceed to the step (5).

NOTE: Wait approximately 10 minutes until the OS is completely started.

(5) Check if the resource group is running normally.
Execute the rgstatus command to confirm whether the resource group is running normally. For the method for confirmation, refer to "Maintenance Tool '2.63 Resource group Status Display (rgstatus)' (MNTT 02-3380)".

(6) Return to the step (c) of "Replacement '1.2.2 Parts replacement only when the node is turned off (single node configuration)' (REP 01-0090)" and execute the rest of the procedures.

Copyright © 2012, 2013, Hitachi, Ltd.

D.1.19 Replacing the Cable

For the cluster configuration, refer to D.1.19.1 Replacing the Cable (cluster configuration).
For the single node configuration, refer to 'D.1.19.2 Replacing the Cable (single node configuration)'.
The various cables indicate that any of 3.5" SAS Cable, SM BUS Cable, Front Panel Cable, DVD SATA Cable, 3.5" FAN Cable Set, Front USB Cable or PS Backboard & Cable connected inside the node.
For the LAN cable connected outside of the node, refer to "Replacement '1.5 Replacing the LAN Cable' (REP 01-0200)", and for FC cable, refer to "Replacement '1.4 Replacing the Fibre Channel Cable' (REP 01-0160)".

D.1.19.1 Replacing the Cable (cluster configuration)

(1) Stop the OS on the target node.
For details about how to stop the OS on a node, refer to "Maintenance Tool '2.28 Terminating the OS of This Side Node (nasshutdown)' (MNTT 02-1740)".

(2) Disconnect all the cables connected to the node itself, because the node is required to be replaced the parts at the support center. All those cables are reconnected after the node is returned. Therefore, be sure to write down the place to connect the cables.

(3) Remove HDD from the node.
The HDD is reinstalled after the node is returned. Therefore, be sure to write down the place to install the HDD.

(4) Because the node is required to be replaced the parts at the support center, wait until the node is returned. When the node is returned, proceed to the next step.

(5) Connect all the cables to the node.

NOTE: When there has been an instruction to let the heartbeat cable and maintenance port cable removed during operation before executing the replacement procedure, do not connect heartbeat cable and the maintenance port cable and just connect the other cables.

(6) Re-install the HDD and turn the Power lamp on.

(7) Confirm that the OS startup of the node is complete.
Refer to "Set Up '1.3 Startup Confirmation of the OS by using KVM' (SETUP 01-0010)" and confirm that the login prompt window is displayed.
If the login prompt window is not displayed and a boot failure window is displayed, the OS startup was not successful because another failure occurred. Refer to 'C.2.4 Diagnosis for OS Boot Failure' and execute the solution to the failure. After the failure is solved, proceed to the step (8).
If the login prompt window is displayed, proceed to the step (8).

(8) Check whether the OS is completely started on the node. To check, execute the peerstatus command on the other (normal) node and check whether the status is [BOOT COMPLETE].
For details about how to check node status, refer to "Maintenance Tool '2.36 Displaying the Status of Other Side Node (peerstatus)' (MNTT 02-2130)".

NOTE: Wait approximately 10 minutes until the OS is completely started.

(9) Return to the step (e) of "Replacement '1.2.1 Parts replacement only when the node is turned off (cluster configuration)' (REP 01-0070)" and execute the rest of the procedures.

Copyright © 2012, 2016, Hitachi, Ltd.

D.1.19.2 Replacing the Cable (single node configuration)

(1) Stop the OS on the target node.
Before stopping the OS of the node, ask the system administrator if the service can be stopped or not. After that confirmation, execute the operation.
For details about how to stop the OS on a node, refer to "Maintenance Tool '2.28 Terminating the OS of This Side Node (nasshutdown)' (MNTT 02-1740)".

(2) Disconnect all the cables connected to the node itself, because the node is required to be replaced the parts at the support center. All those cables are reconnected after the node is returned. Therefore, be sure to write down the place to connect the cables.

(3) Remove HDD from the node.
The HDD is reinstalled after the node is returned. Therefore, be sure to write down the place to install the HDD.

(4) Because the node is required to be replaced the parts at the support center, wait until the node is returned. When the node is returned, proceed to the next step.

(5) Connect all the cables to the node.

(6) Re-install the HDD and turn the Power lamp on.

(7) Confirm that the OS startup of the node is complete.
Refer to "Set Up '1.3 Startup Confirmation of the OS by using KVM' (SETUP 01-0010)" and confirm that the login prompt window is displayed.
If the login prompt window is not displayed and a boot failure window is displayed, the OS startup was not successful because another failure occurred. Refer to 'C.2.4 Diagnosis for OS Boot Failure' and execute the solution to the failure. After the failure is solved, proceed to the step (5).
If the login prompt window is displayed, proceed to the step (5).

NOTE: Wait approximately 10 minutes until the OS is completely started.

(8) Check if the resource group is running normally.
Execute the rgstatus command to confirm whether the resource group is running normally. For the method for confirmation, refer to "Maintenance Tool '2.63 Resource group Status Display (rgstatus)' (MNTT 02-3380)".

(9) Return to the step (c) of "Replacement '1.2.2 Parts replacement only when the node is turned off (single node configuration)' (REP 01-0090)" and execute the rest of the procedures.

Copyright © 2012, 2013, Hitachi, Ltd.

D.1.20 Replacing the BMC

Refer to ‘D.1.9 Replacing the Motherboard’, and execute the replacement of the motherboard.

Copyright © 2012, 2013, Hitachi, Ltd.

This page is for editorial purpose only.

Copyright © 2011, 2013, Hitachi, Ltd.

D.1.21 Replacing the Management Port

Refer to ‘D.1.8 Replacing the GbE-2Port Card’, and execute the replacement of the GbE-2Port card.

Copyright © 2011, 2013, Hitachi, Ltd.

D.1.22 Replacing the Internal RAID Battery

(1) Terminate the OS of the node.
Inform the system administrator of the stop of the service and get allowance to stop the service before stopping OS of the node.
For terminating the OS of the node, refer to "Maintenance Tool '2.28 Terminating the OS of This Side Node (nasshutdown)' (MNTT 02-1740)".

(2) Refer to "Hitachi Advanced Server 8000/RS220xK Maintenance Manual" and replace the Internal RAID Battery.

NOTE: Precautions before the parts replacement

- When replacing Internal RAID Battery, replace it with the instruction described in "Hitachi Advanced Server 8000/RS220xK Maintenance Manual" and confirm the operation after the replacement by using HATP (a program that executes operation confirmation and executes determination when a failure occurs on HA8000 series).
- Depend on the result of HATP, the other possible suspect parts might be replaced. In this case, return to 'C.2.2.2 Failure determination procedure at the single node configuration' and determine the subject parts.

(3) Press the power button on the node.

(4) After the OS is started on the node, check the following.
Check the hardware status. Check whether "ok" is displayed for all items of "InternalRAIDBattery Information" on the screen. (For checking the hardware status, refer to 'B.3.1 Displaying the Hardware Status (hwstatus)'.

Copyright © 2012, 2014, Hitachi, Ltd.

D.1.23 Replacing the USB Board

This is not a part to be replaced.

Copyright © 2012, 2013, Hitachi, Ltd.

D.1.24 Replacing the SFP module

This is not a part to be replaced.

Copyright © 2012, 2014, Hitachi, Ltd.

CONTENTS

D.2 Appendix.A A Node Replacement Procedure

Copyright © 2015, Hitachi, Ltd.

This page is for editorial purpose only.

Copyright © 2015, Hitachi, Ltd.

D.2 Appendix.A A Node Replacement Procedure

HA8000/RS220xK does not support the procedure that replaces one node.

Copyright © 2015, Hitachi, Ltd.

This page is for editorial purpose only.

Copyright © 2015, Hitachi, Ltd.